基礎数学選書

26

編集委員会
矢野 健太郎
国沢 清典
茂木 勇
石原 繁
岩堀 長慶

有限置換群

大阪教育大学教授
理学博士
大山 豪 著

裳華房

編　集　趣　旨

最近の科学技術の発展には誠に目覚しいものがあります．それにつれてその基礎であり，その手段である数学の重要性はますます増大しつつあります．

また一方，いままでは主として科学技術の方面にのみ応用をもっていると思われていた数学が，最近になって実は，人間のあらゆる社会活動を対象とする行動科学の方面にも非常に大きな応用をもっていることが明らかになってまいりました．

このように，科学技術と行動科学の２つの方面からの社会的要求はますます増大する一方ですので，大学における数学教育の比重はますます大きくなりつつあります．

しかしながら誠に残念なことに，大学の講義時間には大きな制限があるために，講義がややもすれば型通りになりがちで，学生の数も毎年増加の一途をたどっていますので，講義だけで学生が将来必要な数学をマスターするということはますます困難になりつつあるのが現状です．

このような状態のもとで，大学の講義を十分に理解し，それを活用する力を十分に身につけるには，初学者の心理も盲点も知りつくしている経験豊かな著者の手になる懇切丁寧な参考書によるのが一番よい方法です．

ややもすれば，大学生相手の書物には読者をつきはなしたような態度が多いのですが，その点を改め，読者諸君が素直に読み進むことができ，しかもそれによって厳密で豊富な知識が身につき，理論に対する真の興味がわいてくるようにと念願して企画されたのが，この「基礎数学選書」であります．

本選書は，以上の趣旨に基づいて，数学の種々の分科を１つ１つ教科書風の堅苦しさから解放された自由な立場から，できるだけ詳細に解説するという目的で，比較的多くの小冊子に分けられています．

読者諸君は，この選書のうちから諸君が必要とされるもの，興味をもたれるものを自由に選ぶことができると思います．

編集委員会は，この選書に入れた項目で，将来数学を活用しようとする人たちに必要なものはほとんど網羅していると信じます．

また，将来それを活用する場合，数学はこの選書に解説されている内容で十分役立つと確信します．

したがって，これらの選書で学習し，それらを書棚においておかれるならば，社会にでて数学を活用する場合にも大いに役立つことを信じて疑わないものであります．

昭和44年8月

矢　野　健太郎

国　沢　清　典

茂　木　　　勇

石　原　　　繁

岩　堀　長　慶

まえがき

数学において，写像という概念は重要な役割をはたしている．それは，一つには与えられた集合の数学的構造を，その集合における写像をとることにより明らかにすることができるということと，もう一つは写像自身が数学的に興味ある構造をもっているということによるものである．

本書では，有限集合における1対1写像――置換という――についての基本的な性質を述べたいと思う．さらに置換の集合は写像の積により群――置換群という――をつくり，群論における重要な一部門である．群論は本来1800年頃Galois 等により，方程式の根の間の置換群としてはじまった．その後1900年頃より，急速に一般的な群論の研究が進められ，現在の有限群論の発展とあいまって，置換群論もその理論をますます深めていった．

本書は，三つの章よりなっている．第1章では必要な予備知識を簡単に述べたが，群論の入門書等に目を通されることをお勧めする．第2章は本書の目的とする章で，置換についての基本的な性質は大体述べたつもりである．第3章では重要な置換群である Mathieu 群について述べ，その構成と共に Mathieu 群が作用する集合の構造との関係という観点からも取り上げた．Mathieu 群は多重可移群の一つであるが，多重可移群の分類については，多くの群論の知識を必要とするので，本書で取り上げることはできなかった．

本書の執筆をお勧め下さった岩堀長慶先生に心から感謝の意を表したい．また，原稿を通読していろいろと助言を下さった大阪大学の平峰豊氏，および本書の執筆校正に関してお世話になった裳華房の遠藤恭平氏，細木周治氏，橋本佳代子氏に深く感謝したい．

昭和56年8月

大　山　　豪

目　　次

1. 予 備 知 識

2. 基 本 的 性 質

3. Mathieu 群

1 予備知識

置換群は当然群の知識を必要とするが，本書では置換群特有の性質を述べることを目的としているので，なるべく群の複雑な定理は使わないように心掛けた．しかしどうしても必要とすることを，有限体，ベクトル空間の簡単な性質と共にこの章であげておく．

なお本書で扱う集合は有限集合，無限集合の区別を必要としない場合も多いが，特に断わらない限り集合はすべて有限集合とする．

§1. 群，部分群

演算（主として積の形で書く）の定義された集合Gが，つぎの条件をみたすとき，Gを**群** (group) という．

（1） 結合法則をみたす．すなわち任意の $a, b, c \in G$ に対して $(ab)c = a(bc)$ が成り立つ．

（2） 単位元をもつ．ここでeがGの単位元であるとは，任意の$x \in G$に対して，$xe = ex = x$ をみたすことである．以下単位元を1と書く．

（3） Gのすべての元は逆元をもつ．ここでyがxの逆元であるとは，$yx = xy = 1$ となることである．xの逆元を x^{-1} と書く．

群Gにおいて，任意の $a, b \in G$ が可換，すなわち $ab = ba$ のときGを**可換群** (commutative group) または**アーベル群** (abelian group) という．

群Gの元の個数をGの**位数** (order) といい，$|G|$と書く．ここで一般に集合Sの元の個数を同じように$|S|$と書く．

群Gにおいて，位数が有限のとき**有限群**，無限のとき**無限群**という．本書においては群といえば，特に断わらない限り有限群を意味することとする．

群 G の部分集合HがGと同じ演算により群となるとき，HをGの**部分群**

(subgroup) といい，$H \leqq G$ または $G \geqq H$ と書く．特に $H \neq G$ のとき，H を G の **真部分群** (proper subgroup) といい，必要があれば $H \lneqq G$ と書く．また単位元 1 のみからなる部分群 $\{1\}$ を単に 1 と書くことが多い．

X, Y を群 G の部分集合とするとき，

$$XY = \{xy \mid x \in X, y \in Y\}$$
$$X^{-1} = \{x^{-1} \mid x \in X\}$$

と定義する．また $x \in G$ に対して $\{x\}Y$ を xY, $Y\{x\}$ を Yx と書く．このとき $|xY| = |Yx| = |Y|$ である．

群 G の元 x の n 個の積を x^n と書く．また $(x^n)^{-1} = (x^{-1})^n$ だから $x^{-n} = (x^n)^{-1}$, $x^0 = 1$ とする．

S を群 G の部分集合とするとき，$\{x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} \mid x_i \in S,\ n_i$ は整数$\}$ は G の部分群を作る．これを **S で生成された群** といい $\langle S \rangle$ と書く．また S を $\langle S \rangle$ の **生成系**，S の元を $\langle S \rangle$ の **生成元** という．特に $S = \{a_1, a_2, \cdots, a_m\}$ に対して，$\langle S \rangle$ を $\langle a_1, a_2, \cdots, a_m \rangle$ とも書く．

H を群 G の部分群とする．$a \in G$ に対して Ha を a を含む H の（または H を法とする）**左剰余類** (left coset)，aH を a を含む H の（または H を法とする）**右剰余類** (right coset) という．群 G は互いに共通な元を含まない（互いに素という）部分群 H の左剰余類の和集合 $G = Ha_1 + Ha_2 + \cdots + Ha_n$ として表される．これを G の H による **左分解** といい，集合 $\{Ha_1, Ha_2, \cdots, Ha_n\}$ を G/H と書く．また H の右剰余類による G の分解を **右分解** という．ここでつぎの定理 1.1 より，左または右分解に現れる左剰余類と右剰余類の個数は等しいから，これを G における H の **指数** (index) といい $|G:H|$ または $|G/H|$ と書く．

定 理 1.1 H を群 G の部分群とするとき

$$|G| = |G:H| \cdot |H|$$

である．

［証 明］ $G = Ha_1 + Ha_2 + \cdots + Ha_n$ を G の H による左分解とすると $|G:H| = n$ である．一方 $|H| = |Ha_i|$ $(i = 1, 2, \cdots, n)$ であるから，$|G| = |G:H| \cdot |H|$ がえられる． □

aを群Gの元とするとき，$\langle a\rangle$ をaで生成された**巡回群** (cyclic group), aを巡回群 $\langle a\rangle$ の生成元という．また $|\langle a\rangle|$ をaの**位数**という．

定理 1.2 巡回群はその位数の約数を位数とする部分群をただ1つもち，それはまた巡回群である．

［**証明**］ 巡回群 $G=\langle a\rangle$ の位数を n, HをGの部分群 ($\neq 1$) とする．lを $a^l\in H$ である最小の正整数とし，Hの任意の元 a^k に対して $k=ql+r,\ 0\leqq r\lneqq l$ とする．このとき

$$a^r=a^{k-ql}=a^k\cdot(a^l)^{-q}\in H$$

である．したがってlの最小性により $r=0$, $a^k=(a^l)^q$ となり，Hは巡回群 $\langle a^l\rangle$ である．

つぎに m ($\gneqq 0$) をnの約数とすると，$\langle a^{n/m}\rangle$ は位数mの部分群である．いまKを位数mのGの任意の部分群とするとき，上の証明における整数 l' が存在して $K=\langle a^{l'}\rangle$ となる．一方 $a^n=1\in\langle a^{l'}\rangle$ であるから，上で示したように $n=l'q'$ となる．したがってKの位数は q' となり，$q'=m$ である．すなわち $l'=n/m$ となり，Kは $\langle a^{n/m}\rangle$ に一致する． □

H, K を群Gの部分群とする．$x\in G$ に対して，HxK をxを含む (H, K) による**両側剰余類** (double coset) という．このときGは，互いに素な両側剰余類の和 $G=Hx_1K+Hx_2K+\cdots+Hx_nK$ に分解される．

定理 1.3 Hを群Gの部分集合とする．Hの任意の元 x, y に対して $xy\in H$ であれば，HはGの部分群である．

［**証明**］ 任意の $x, y\in H$ に対して $xy\in H$ であるから，$xH\subseteqq H$ である．ここでHは有限集合であるから，$|xH|=|H|$で，したがって $xH=H$ となる．これより $x\in H$ であるから，$xy=x$ となる元yがHに存在し，yは単位元1である．さらに $xH=H\ni 1$ より $xx'=1$ となる元 x' がHに存在し，x' はxの逆元 x^{-1} である．以上よりHはGの部分群となる． □

定理 1.4 H, K を群Gの部分群とすると，$|HK|=|H|\cdot|K|/|H\cap K|$ である．特に $HK=KH$ であれば HK もGの部分群である．

［**証明**］ HK はHの互いに素な左剰余類の和集合として

$$HK=Hk_1+Hk_2+\cdots+Hk_r,\qquad k_i\in K\ (i=1,2,\cdots,r)$$

と書ける．このとき

$$K = (H \cap K)k_1 + (H \cap K)k_2 + \cdots + (H \cap K)k_r$$

はKの部分群$H \cap K$による左分解である. なぜならば, 任意の $k \in K$ に対して $K \subseteqq HK$ であるから, $k \in Hk_i$ となる $k_i \in K$ が存在する. このとき $kk_i^{-1} \in H \cap K$ となり $k \in (H \cap K)k_i$ である. したがって, $K = \bigcup_{i=1}^{r} (H \cap K)k_i$である.

いま $(H \cap K)k_i = (H \cap K)k_j$ とすると, $k_i k_j^{-1} \in H \cap K \leqq H$ より $Hk_i = Hk_j, k_i = k_j$ となり, 上のKの分解は $H \cap K$ による左分解である.

したがって定理 1.1 より $r = |K : K \cap H| = |K| / |H \cap K|$ となり, $|HK| = |H| \cdot r = |H| \cdot |K| / |H \cap K|$ をうる.

いま $HK = KH$ とする. このとき $(HK)(HK) = H(KH)K = H(HK)K = HK$ となり, 定理 1.3 より HK は部分群を作る. □

§2. 正規部分群

群 G の元 x (または部分集合 X) に対して, $y \in G$ により $y^{-1}xy$ (または $y^{-1}Xy$) を作ることを x(またはX) をyで**変換する**といい, $y^{-1}xy = x^y$, $y^{-1}Xy = X^y$ と書く.

Hを群Gの部分群とする. Gの元 x_1, x_2 (または部分集合 X_1, X_2) に対して $y \in H$ が存在して, $x_1^y = x_2$ (または$X_1^y = X_2$) になるとき, x_1 と x_2 (または X_1 と X_2) はHで**共役** (conjugate) または**H-共役**であるという. 特に G-共役のときは単に共役ということが多い.

集合 S の元の間に関係 $\sim$ が定義されて, つぎの 3 つの条件 (同値律という)

反射律 $a \sim a$

対称律 $a \sim b \Rightarrow b \sim a$

推移律 $a \sim b, b \sim c \Rightarrow a \sim c$

をみたすとき, この関係$\sim$を**同値関係**という. また $\{x \in S | x \sim a\}$ をaを含む**同値類**という. このときSは互いに素な同値類のいくつかの和集合になり, このSの分割を**類別**という. §1 で述べた群Gの部分群Hによる左分解は, $x, y \in G$ に対して関係 $x \sim y$ を $xy^{-1} \in H$ により定義したときの類別である.

群Gの元の間の共役の関係は同値関係である. したがって共役によるGの元

の同値類を**共役類** (conjugacy class) という.

群Gにおいて $\{a \in G \mid a^x = a\ (^\forall x \in G)\}$ はGの部分群を作る. これをGの**中心** (center) といい, $Z(G)$ と書く.

群Gの共役類を $C_1 = \{1\}, C_2, \cdots, C_r$, $|C_1| = 1$, $|C_i| = n_i$ $(i = 2, 3, \cdots, r)$ とすると

$$|G| = 1 + n_2 + \cdots + n_r$$

である. これをGの**類等式** (class equation) という. また $Z(G)$ の元はそれぞれ1つで, 1つの共役類を作る. したがって共役類の番号を適当につけかえて, $Z(G) = \{z_1 = 1, z_2, \cdots, z_s\}$, $\{z_i\} = C_i$ $(i = 1, 2, \cdots, s)$ とすると

$$|G| = s + n_{s+1} + \cdots + n_r$$

である. これもGの類等式という.

Xを群Gの部分集合, HをGの部分群とするとき, $\{a \in H \mid X^a = X\}$ をHにおけるXの**正規化群** (normalizer) といい $N_H(X)$ と書く. $N_H(X)$ はHの部分群である. $N_G(X)$ を単に $N(X)$ と書くときもある. また $\{a \in H \mid x^a = x, (^\forall x \in X)\}$ をHにおけるXの**中心化群** (centralizer) といい $C_H(X)$ と書く. $C_H(X)$ もHの部分群である. $C_G(X)$ を単に $C(X)$ と書くときもある.

群 G の部分群 H が $N_G(H) = G$ のとき, HをGの**正規部分群** (normal subgroup) といい $H \trianglelefteq G$ または $G \trianglerighteq H$ と書く. 群 $G(\neq 1)$ がGと1以外に正規部分群をもたないとき, Gを**単純群** (simple group) という.

H を群 G の正規部分群とする. このとき H を法とする G の剰余類の集合 $\{Hx \mid x \in G\}$ は, $(Hx)(Hy) = Hxy$ により演算が定義され, この演算により群になる. これをHを法とするGの**剰余群** (factor group) といい G/H と書く.

定理 2.1 xを群Gの元, Xを群Gの部分集合とする.

(1) xを含むGの共役類の元の個数は $|G : C_G(x)|$ に等しい.

(2) Xに共役なGの部分集合の個数は $|G : N_G(X)|$ に等しい.

[証 明] $N_G(X)$ を法とするGの左分解を

$$G = N_G(X)a_1 + N_G(X)a_2 + \cdots + N_G(X)a_n$$

とする．任意の $x \in N_G(X)$ に対して $X^{xa_i} = X^{a_i}$ であるから，$X^{N_G(X)a_i} = \{X^{xa_i} | x \in N_G(X)\} = \{X^{a_i}\}$ である．いま $X^{a_i} = X^{a_j}$ とすると $X^{a_i a_j^{-1}} = X,\ a_i a_j^{-1} \in N_G(X)$ となり，$a_i = a_j$ である．したがってXと共役なGの部分集合は $X^{a_1}, X^{a_2}, \cdots, X^{a_n}$ で，その個数は $|G:N_G(X)|$ に等しい．

特に $X=\{x\}$ のとき，$N_G(X)=C_G(x)$ だから（1）が成り立つ． □

定 理 2.2 群Gの指数 2 の部分群は，Gの正規部分群である．

［証 明］ HをGの指数 2 の部分群とする．任意の $x \in G-H$ に対して $G=H+Hx=H+xH$ であるから，$Hx=xH, H^x=H$ となり $H \trianglelefteq G$ である． □

位数が素数 p のべきである群を **p-群** （p-group）という．また元（$\neq 1$）の位数がすべて p である可換 p-群を，**基本可換群** (elementary abelian group) という．特に位数 4 の基本可換群を **4 元群** (four group) という．

定 理 2.3 P を p-群（$\neq 1$）とする．このときPの中心 $Z(P) \neq 1$ である．またQをPの真部分群とすると，$Q \subsetneqq N_P(Q)$ である．

［証 明］ Pの類等式 $|P|=|Z(P)|+n_1+n_2+\cdots+n_k$ をとる．ここで $n_i\ (i=1, 2, \cdots, k)$ は $a_i \notin Z(P)$ を含む共役類 $C(a_i)$ の元の個数である．このとき定理 2.1 (1) より，$n_i=|P:C_P(a_i)|$ で $C_P(a_i) \subsetneqq P$ であるから，n_i は p のべき（$\neq 1$）である．したがって上の類等式において，$|P|$ も p のべき（$\neq 1$）であるから，$|Z(P)|$ も p のべき（$\neq 1$）になり，$Z(P) \neq 1$ である．

つぎにQによる両側剰余類へのPの分解を，$P=Q+Qx_1Q+Qx_2Q+\cdots+Qx_lQ$ とする．ここで Qx_iQ はQの左剰余類の和集合で，その個数は $|Qx_iQ|/|Q|$ に等しい．定理 1.4 より，

$$|Qx_iQ|=|x_i^{-1}Qx_iQ|=|Q^{x_i}Q|=|Q^{x_i}|\cdot|Q|/|Q^{x_i}\cap Q|$$

であるから，$|Qx_iQ|/|Q|=|Q^{x_i}|/|Q^{x_i}\cap Q|$ となり，Q^{x_i} は p-群であることから $|Q^{x_i}|/|Q^{x_i}\cap Q|=p^{r_i}\ (r_i \geqq 0)$ となる．したがって上の両側分解より $|P:Q|=1+p^{r_1}+p^{r_2}+\cdots+p^{r_l}$ である．ここで左辺はpのべき（$\neq 1$）であるから，$p^{r_i}=1$ となる r_iが存在する．このとき $Q^{x_i}=Q^{x_i}\cap Q$，すなわち $Q^{x_i}=Q,\ x_i \in N_P(Q)$ となり，$Q \subsetneqq N_P(Q)$ である． □

群 $G_1, G_2, \cdots, G_n$ の直積集合を $G=\{(a_1, a_2, \cdots, a_n) | a_i \in G_i\}$ とする．Gの元の間の積を

$$(a_1, a_2, \cdots, a_n)\ (b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$$

により定義すると，Gは群になる．このときGを $G_1, G_2, \cdots, G_n$ の**直積**（direct product）といい，$G = G_1 \times G_2 \times \cdots \times G_n$ と書く．

また群Gの部分群 $H_1, H_2, \cdots, H_n$ がつぎの条件をみたすとき，Gは部分群 $H_1, H_2, \cdots, H_n$ の直積であるといい，$G = H_1 \times H_2 \times \cdots \times H_n$ と書く．

（1）$H_i \trianglelefteq G \qquad (i = 1, 2, \cdots, n)$

（2）$G = H_1H_2\cdots H_n$

（3）$(H_1H_2\cdots H_{i-1}) \cap H_i = 1 \qquad (i = 2, 3, \cdots, n)$

定 理 2.4 位数 p^n（pは素数）の基本可換群は，位数 p の巡回群n個の直積である．

［**証 明**］ $P-\{1\}$ の元 a_1 をとると，$\langle a_1\rangle$ は位数pでPの正規部分群である．$P \gneqq \langle a_1\rangle$ であれば，$P-\langle a_1\rangle$ の元 a_2 をとると，$\langle a_2\rangle$ は位数pのPの正規部分群で，$\langle a_1, a_2\rangle$ は直積 $\langle a_1\rangle \times \langle a_2\rangle$ で，位数 p^2 である．以下この操作を続けることにより，$P = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_n\rangle$ となる． □

§3. 準同型

集合Aから集合 B への写像φを $\varphi : A \to B$ と書き，φにより $a \in A$ が $b \in B$ にうつることを $a \mapsto b$ と書く．φ による $a \in A$ の像を a^φ と書き，$A^\varphi = \{a^\varphi | a \in A\}$ とする．また $b \in B$ に対して $b^{\varphi^{-1}} = \{a \in A | a^\varphi = b\}$ とし，$B' \subseteqq B$ に対しては $B'^{\varphi^{-1}} = \{a \in A | a^\varphi \in B'\}$ とする．$A^\varphi = B$ のときφを**全射**，任意の $a \in A$ に対して $(a^\varphi)^{\varphi^{-1}} = \{a\}$ のときφを**単射**といい，φが全射で単射のとき**全単射**または**上への1対1写像**という．

写像 $\varphi{:}A \to B$ と写像 $\psi{:}B \to C$ との積を $\varphi\psi$ と書く．このとき $a \in A$ に対して，$a^{\varphi\psi} = (a^\varphi)^\psi$ である．

群Gから群 G' への写像φが

$$(xy)^\varphi = x^\varphi y^\varphi, \qquad (^\forall x, y \in G)$$

をみたすとき，φを G から G' への**準同型（写像）**（homomorphism）という．また $1'$ を G' の単位元とするとき，$1'^{\varphi^{-1}} = \{x \in G | x^\varphi = 1'\}$ をφの**核**（kernel）といい $\ker\varphi$ と書く．定理 3.1 (2) で示すように，$\ker\varphi$ はGの

正規部分群であり，特に $\ker\varphi=1$ のときφは単射である．

Nを群Gの正規部分群とする．写像 $\varphi: G\to G/N, x\mapsto Nx$ はGから G/N の上への準同型である．この写像φをGから G/N への**自然準同型**（canonical homomorphism）という．

φを群Gから群 G' への準同型とする．φが全単射のとき，すなわち $G^{\varphi}=G', \ker\varphi=1$ のとき，GとG' は**同型**であるといい $G\cong G'$ と書く．またφをGから G' の上への**同型（写像）**（isomorphism）という．

定理 3.1 φを群Gから群 G' への準同型とする．

（1） $H\leq G$ のとき，$H^{\varphi}\leq G'$ である．さらに $H\trianglelefteq G$ であれば，$H^{\varphi}\trianglelefteq G^{\varphi}$ である．

（2） $H'\leq G'$ のとき，$H'^{\varphi^{-1}}\leq G$ である．さらに $H'\trianglelefteq G'$ であれば，$H'^{\varphi^{-1}}\trianglelefteq G$ である．

［証明］（1） 任意の $x', y'\in H^{\varphi}$ に対して，$x^{\varphi}=x', y^{\varphi}=y'$ となる $x, y\in H$ が存在する．このとき $x'y'=x^{\varphi}\cdot y^{\varphi}=(xy)^{\varphi}\in H^{\varphi}$ となり，定理 1.3 より $H^{\varphi}\leq G'$ である．さらに $H\trianglelefteq G$ とするとき，任意の $x^{\varphi}\in G^{\varphi}$ $(x\in G)$ に対して $(x^{\varphi})^{-1}=(x^{-1})^{\varphi}$ であるから $(x^{\varphi})^{-1}H^{\varphi}x^{\varphi}=(x^{-1}Hx)^{\varphi}=H^{\varphi}$ となり，$H^{\varphi}\trianglelefteq G^{\varphi}$ である．

（2） 任意の $x, y\in H'^{\varphi^{-1}}$ に対して $x^{\varphi}, y^{\varphi}\in H'$ であるから，$(xy)^{\varphi}=x^{\varphi}y^{\varphi}\in H', xy\in H'^{\varphi^{-1}}$ となり，定理 1.3 より $H'^{\varphi^{-1}}\leq G$ である．さらに $H'\trianglelefteq G'$ とするとき，任意の $x\in G$ に対して

$$(x^{-1}H'^{\varphi^{-1}}x)^{\varphi}=(x^{\varphi})^{-1}(H'^{\varphi^{-1}})^{\varphi}x^{\varphi}\subseteq(x^{\varphi})^{-1}H'x^{\varphi}=H',\qquad x^{-1}H'^{\varphi^{-1}}x\leq H'^{\varphi^{-1}}$$

となり，$H'^{\varphi^{-1}}\trianglelefteq G$ である． □

定理 3.2 φをGから G' の上への準同型とし，$N=\ker\varphi$ とする．

（1）（準同型定理） $G/N\cong G'$ である．

（2） $X\subseteq G$ に対して $(X^{\varphi})^{\varphi^{-1}}=XN$ である．

（3）（対応定理） $\{H\mid N\leq H\leq G\}$ と $\{H'\mid H'\leq G'\}$ との間に，Hと H^{φ} が対応する1対1対応が存在する．特にこの対応において，Nを含むGの正規部分群と G' の正規部分群が対応する．

（4）（第1同型定理） $H'\trianglelefteq G'$ に対して $G'/H'\cong G/H'^{\varphi^{-1}}$ である．

［証明］（1）$Nx,\ Ny\in G/N$ が $Nx=Ny$ であれば，$xy^{-1}\in N,\ (xy^{-1})^{\varphi}=1'$．

$x^{\varphi}(y^{\varphi})^{-1}=1'$ となり $x^{\varphi}=y^{\varphi}$ である．よって，写像 $\bar{\varphi}:G/N\to G'$ を $(Nx)^{\bar{\varphi}}=x^{\varphi}$ により定義できて，$\bar{\varphi}$ は明らかに全射である．このとき任意の $Nx, Ny\in G/N$ に対して，

$$(Nx\cdot Ny)^{\bar{\varphi}}=(Nxy)^{\bar{\varphi}}=(xy)^{\varphi}=x^{\varphi}y^{\varphi}=(Nx)^{\bar{\varphi}}(Ny)^{\bar{\varphi}}$$

であるから，$\bar{\varphi}$ は準同型である．つぎに

$$\ker\bar{\varphi}=\{Nx\in G/N\,|\,(Nx)^{\bar{\varphi}}=1'\}=\{Nx\in G/N\,|\,x^{\varphi}=1'\}=\{Nx\in G/N\,|\,x\in N\}=N$$

より $\bar{\varphi}$ は同型となり，$G/N\cong G'$ である．

（2） $(XN)^{\varphi}=X^{\varphi}N^{\varphi}=X^{\varphi}$ であるから，$XN\subseteqq(X^{\varphi})^{\varphi^{-1}}$ である．任意の $x\in(X^{\varphi})^{\varphi^{-1}}$ に対して $x^{\varphi}\in X^{\varphi}$ であるから，$x^{\varphi}=y^{\varphi}$ となる $y\in X$ が存在する．したがって，$(y^{-1}x)^{\varphi}=1'$ より $y^{-1}x\in N$, $x\in yN\subseteqq XN$ となり，$XN=(X^{\varphi})^{\varphi^{-1}}$ である．

（3） 定理 3.1（1）より $H^{\varphi}\leqq G'$ であるから，写像 $f:\{H\,|\,N\leqq H\leqq G\}\to\{H'\,|\,H'\leqq G'\}$ を $H\mapsto H^{\varphi}$ により定義する．任意の $H'\leqq G'$ に対して $H=H'^{\varphi^{-1}}$ とおくと，定理 3.1（2）および上の（2）より $N\leqq H\leqq G$ である．したがって $H^f=H^{\varphi}=(H'^{\varphi^{-1}})^{\varphi}=H'$ となり，f は全射である．つぎにNを含むGの部分群 H_1, H_2 に対して $H_1{}^f=H_2{}^f$ とする．このとき $H_1{}^{\varphi}=H_2{}^{\varphi}, (H_1{}^{\varphi})^{\varphi^{-1}}=(H_2{}^{\varphi})^{\varphi^{-1}}$ となり，（2）より $H_1N=H_2N$, すなわち $H_1=H_2$ となり，f は全単射である．

また正規部分群については定理3.1より成り立つ．

（4） 写像 $f:G'\to G'/H'$ を自然準同型とするとき，写像 $\varphi f:G\to G'/H'$ は全射準同型となる．ここで

$$\ker\varphi f=\{x\in G\,|\,x^{\varphi f}=\bar{1}:\bar{1}\text{ は }G'/H'\text{ の単位元}\}=\{x\in G\,|\,x^{\varphi}\in H'\}=H'^{\varphi^{-1}}$$

となり，（1）より $G'/H'\cong G/H'^{\varphi^{-1}}$ である．□

定理 3.3（第2同型定理） $H\leqq G$, $N\trianglelefteq G$ に対して $HN/N\cong H/H\cap N$ である．

［**証明**］ 定理 1.4 より $HN\leqq G$ である．自然準同型 $\varphi:G\to G/N$ において $H^{\varphi}=HN/N$ である．したがって写像 $\bar{\varphi}:H\to HN/N, h\mapsto h^{\varphi}$ は全射準同型となる．ここで $\ker\bar{\varphi}=\{x\in H\,|\,x^{\bar{\varphi}}=\bar{1}\}=\{x\in H\,|\,x\in N\}=H\cap N$ であるから，定理 3.2（1）より $HN/N\cong H/H\cap N$ である．□

群GからGの上への同型をGの**自己同型**（automorphism）という．Gの自己同型全体は写像の積により群を作る．これをGの**全自己同型群**といい $\mathrm{Aut}\,G$ と書く．$\mathrm{Aut}\,G$ の部分群を**自己同型群**という．また $a\in G$ による G の自己同型 $x\mapsto a^{-1}xa=x^a$ を，aによるGの**内部自己同型**（inner

automorphism）という．G の内部自己同型全体は $\mathrm{Aut}\,G$ の正規部分群を作る．これを G の**内部自己同型群**といい $\mathrm{Inn}\,G$ と書く．さらに剰余群 $\mathrm{Aut}\,G/\mathrm{Inn}\,G$ をGの**外部自己同型群**といい $\mathrm{Out}\,G$ と書く．

群Gの部分群Hで，任意の $\varphi\in\mathrm{Aut}\,G$ に対して $H^{\varphi}=H$ のとき，HをGの**特性部分群**（characteristic subgroup）という．特性部分群は正規部分群である．

定 理 3.4 巡回群の自己同型群は可換群である．

［証 明］ 巡回群を $G=\langle a\rangle$ とし，任意の $\alpha, \beta\in\mathrm{Aut}\,G$ をとる．Gの自己同型はGの生成元 a の像により一意的に決まる．いま $a^{\alpha}=a^{r}$，$a^{\beta}=a^{s}$ とすると $a^{\alpha\beta}=(a^{\alpha})^{\beta}=(a^{r})^{\beta}=a^{rs}$，$a^{\beta\alpha}=(a^{\beta})^{\alpha}=(a^{s})^{\alpha}=a^{sr}$ となるから，$\alpha\beta=\beta\alpha$ となり $\mathrm{Aut}\,G$ は可換群である．□

定 理 3.5 Hを群Gの部分群とすると，$N_G(H)/C_G(H)$ はHの自己同型群とみなすことができる．特に $G/Z(G)\cong\mathrm{Inn}\,G$ である．

［証 明］ $a\in N_G(H)$ により G の内部自己同型が定義できるが，これをHに制限してHの自己同型 $\bar{a}:H\to H$，$x\mapsto x^{a}$ が定義できる．このとき写像 $\varphi: N_G(H)\to\mathrm{Aut}\,H$，$a\mapsto\bar{a}$ は準同型で，

$$\ker\varphi=\{a\in N_G(H)\,|\,\bar{a}=1\}=\{a\in N_G(H)\,|\,x^{a}=x\ (\forall x\in H)\}=C_G(H)$$

であるから，定理 3.2（1）より $N_G(H)/C_G(H)\cong N_G(H)^{\varphi}\leqq\mathrm{Aut}\,H$ である．したがって $a\in N_G(H)$ のH に対する作用を $\bar{a}$ で定義することにより，$N_G(H)/C_G(H)$ はHの自己同型群とみなすことができる．

特に $H=G$ のとき，$N_G(G)^{\varphi}=G^{\varphi}=\mathrm{Inn}\,G$ であるから $N_G(G)/C_G(G)=G/Z(G)\cong\mathrm{Inn}\,G$ である．□

§4. 交換子群

群Gの元xとyの**交換子**とは $x^{-1}y^{-1}xy$ をいい $[x, y]$ と書く．したがって $[x,y]=1$ のとき，xとyは可換である．またGの部分集合 X, Y に対して，$\langle[x,y]\,|\,x\in X,\ y\in Y\rangle$ をXとYの**交換子群**（commutator subgroup）といい $[X, Y]$ と書く．特に $[G, G]$ を G の交換子群といい，$D(G)$ とも書く．

定 理 4.1 H, K を群Gの正規部分群とする．

（1） $[H,K]\leqq H\cap K$，$[H,K]\trianglelefteq G$ である．

（2） G/H が可換群であれば $[G,G]\leqq H$ であり，逆も成り立つ．

［証 明］（1） 任意の $h\in K$，$k\in K$ に対して，$H\trianglelefteq G$，$K\trianglelefteq G$ であるから，$[h,k]=h^{-1}k^{-1}hk=h^{-1}h^{k}=(k^{-1})^{h}k$ より $[h,k]\in H\cap K$ となり，$[H,K]\leqq H\cap K$ である．また任意の $x\in G$ に対して

$$[h,k]^{x}=(h^{-1}k^{-1}hk)^{x}=(h^{x})^{-1}(k^{x})^{-1}h^{x}k^{x}=[h^{x},k^{x}]\in[H,K]$$

であるから，$[H,K]\trianglelefteq G$ である．

（2） x,y を G の任意の元とするとき，

$$\begin{aligned}G/H \text{ が可換群} &\Longleftrightarrow (Hx)^{-1}(Hy)^{-1}(Hx)(Hy)=H\\ &\Longleftrightarrow Hx^{-1}y^{-1}xy=H\Longleftrightarrow x^{-1}y^{-1}xy\in H\Longleftrightarrow[G,G]\leqq H\end{aligned}$$

である．□

群 G において G の部分群の列 $G=D_0(G)\geqq D_1(G)\geqq\cdots$，$D_1(G)=D(G)$，$D_i(G)=D(D_{i-1}(G))$ を，G の**交換子群列** (derived series) という．ここで $D_r(G)=1$ となる r が存在するとき，G を**可解群** (solvable group) という．

群 G において G の部分群の列 $G=\Gamma_0(G)\geqq\Gamma_1(G)\geqq\cdots$，$\Gamma_1(G)=[G,G]$，$\Gamma_i(G)=[G,\Gamma_{i-1}(G)]$ を，G の**降中心列** (lower central series) という．ここで $\Gamma_r(G)=1$ となる r が存在するとき，G を**べき零群** (nilpotent group) という．

§5. 体，ベクトル空間

加法と乗法の 2 つの演算が定義された集合 K がつぎの条件をみたすとき，K を**体** (field) という．

（1） K は加法に関して可換群である．加法の単位元を 0 と書く．

（2） $K^{\#}=K-\{0\}$ は乗法に関して可換群である．

（3） 分配法則をみたす．すなわち任意の $\lambda,\mu,\nu\in K$ に対して，$\lambda(\mu+\nu)=\lambda\mu+\lambda\nu$ である．

乗法に関する群 $K^{\#}$ を K の**乗法群**という．

体 K から体 K' への写像 φ が，任意の $\lambda,\mu\in K$ に対して

（1） $(\lambda+\mu)^{\varphi}=\lambda^{\varphi}+\mu^{\varphi}$

（2） $(\lambda\mu)^{\varphi}=\lambda^{\varphi}\mu^{\varphi}$

をみたすとき，φ をKから K' への**準同型**という．特に φ が全単射のとき φ を**同型**という．またこのとき，Kと K' は同型であるといい $K\cong K'$ と書く．KからK自身の上への同型をKの**自己同型**という．Kの自己同型全体は写像の積により群を作る．これをKの**全自己同型群**といい $\mathrm{Aut}\,K$ と書く．

有限個の元からなる体を**有限体**という．

この節における定理の証明には，体等の性質に関する知識を少し必要とするので，証明ぬきで定理を述べることにする．

定理 5.1 有限体の元の個数はある素数のべきである．さらに与えられた素数のべきを元の個数とする有限体は，ただ1つ（同型なものは同一視して）存在する．

したがって素数pに対して，元の個数が p^n 個である有限体を $GF(p^n)$ と書き，pを**標数**という．特に $GF(p)$ を標数pの**素体**という．$GF(p)$ は eを乗法の単位元とするとき，$\{0, e, 2e, \cdots, (p-1)e\}$ である．また $GF(p^n)$ において $p\lambda=0, (\lambda\pm\mu)^{p^r}=\lambda^{p^r}\pm\mu^{p^r}$ $(^\forall\lambda, \mu\in GF(p^n))$ が成り立つ．

定理 5.2 $GF(p^n)$ の乗法群 $GF(p^n)^\#$ は，位数 p^n-1 の巡回群である．

定理 5.3 $\mathrm{Aut}\,GF(p^n)$ は位数nの巡回群 $\langle\theta\rangle$

$$\theta:\ \xi\mapsto\xi^p \qquad (^\forall\xi\in GF(p^n))$$

である．

Kを体とし，集合Vがつぎの条件をみたすとき，VをK上の**ベクトル空間** (vector space)，Vの元を**ベクトル**という．

（1） Vに加法が定義されて，可換群をなす．

（2） 任意の $\lambda\in K$ と $v\in V$ に対して，λとvのスカラー積 $\lambda v\in V$ が定義されてつぎをみたす．任意の $\lambda, \mu\in K$，$u, v\in V$ に対して

(2.1) $\lambda(u+v)=\lambda u+\lambda v$

(2.2) $(\lambda+\mu)v=\lambda v+\mu v$

(2.3) $(\lambda\mu)v=\lambda(\mu v)$

(2.4) $K^\#$ の単位元1に対して $1v=v$ である.

VをK上のベクトル空間とする. $v_1, v_2, \cdots, v_r \in V$ に対して, $\lambda_1 v_1+\lambda_2 v_2+\cdots+\lambda_r v_r$ ($\lambda_i \in K$) を $v_1, v_2, \cdots, v_r$ の**1次結合**という. また $\{\lambda_1 v_1+\lambda_2 v_2+\cdots+\lambda_r v_r \mid \lambda_i \in K, i=1,2,\cdots,r\}$ はVの部分集合でベクトル空間, すなわちVの部分ベクトル空間を作る. これを $\langle v_1, v_2, \cdots, v_r\rangle$ と書く.

また, $\lambda_1 v_1+\lambda_2 v_2+\cdots+\lambda_r v_r=0$ ならば, つねに $\lambda_1=\lambda_2=\cdots=\lambda_r=0$ のとき, $v_1, v_2, \cdots, v_r$ は**1次独立**であるという.

K上のベクトル空間Vにおいて, $v_1, v_2, \cdots, v_n \in V$ がつぎの条件

(1) $V=\langle v_1, v_2, \cdots, v_n\rangle$

(2) $v_1, v_2, \cdots, v_n$ は1次独立である.

をみたすとき, $v_1, v_2, \cdots, v_n$ をVの**基**という. Vがn個のベクトルからなる基をもつとき, Vの基のとり方にかかわらず, 基を作るベクトルの個数はn個である. したがって, このときVの**次元**はnであるといい, VがK上のn次元ベクトル空間であることを示すため, $V=V(n,K)$ とも書く.

定理 5.4 Vを体K上のn次元ベクトル空間とする. ベクトル $v_1, v_2, \cdots, v_r \in V$ が1次独立であれば, Vに $v_1, v_2, \cdots, v_r$ を含む基 $\{v_1, v_2, \cdots, v_r, v_{r+1}, \cdots, v_n\}$ が存在する.

2　基本的性質

§1. 置換

Ωを有限集合とする．ΩからΩの上への1対1写像をΩ上の**置換**（permutation）という．集合Ωの元をΩの**文字**または**点**という．$|\Omega|=n$のとき，Ωの文字に適当な順序で番号をうち，$\Omega=\{1,2,\cdots,n\}$とすることが多い．本書では特に断わらない限り，$\Omega=\{1,2,\cdots,n\}$とする．

xをΩ上の置換とするとき，Ωの文字iのxによる像をi^xと書く．このときΩの文字iとxによる像i^xを用いて

$$x=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^x & 2^x & \cdots & n^x\end{pmatrix}$$

と書く．また簡単に$x=\begin{pmatrix}i\\ i^x\end{pmatrix}$と書くこともある．

例1. $\Omega=\{1,2,3,4\}$, $1^x=2$, $2^x=3$, $3^x=1$, $4^x=4$ のとき，$x=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}$ と書く．また文字の並べかたを変えて$x=\begin{pmatrix}2 & 4 & 1 & 3\\ 3 & 4 & 2 & 1\end{pmatrix}$等と書いてもよい．

Ω上の2つの置換$x=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^x & 2^x & \cdots & n^x\end{pmatrix}$，$y=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^y & 2^y & \cdots & n^y\end{pmatrix}$に対して，$x$と$y$との積　xyを

$$xy=\begin{pmatrix}1 & 2 & \cdots & n\\ 1^x & 2^x & \cdots & n^x\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ 1^y & 2^y & \cdots & n^y\end{pmatrix}=\begin{pmatrix}1 & 2 & \cdots & n\\ (1^x)^y & (2^x)^y & \cdots & (n^x)^y\end{pmatrix}$$

により定義する．ここでΩの文字iのxyによる像を，$x(y(i))=(i^y)^x$と定義する場合もあるが本書では用いない．

例2. $x=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$，$y=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$のとき，$xy=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$ $=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$である．

Ω上の置換全体の集合は，上で定義された積に関して群を作る．これをΩ上の**対称群**（symmetric group）という．$|\Omega|=n$ のとき，n次の対称群といい，S^Ω または S_n と書く．S_n の単位元は恒等写像$\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}$で，$\Omega$の文字1と混同しない限り1と書く．$x\in S_n$ の逆元 x^{-1} はxの逆写像$\begin{pmatrix}1^x & 2^x & \cdots & n^x\\ 1 & 2 & \cdots & n\end{pmatrix}$である．

$\Omega=\{1, 2, \cdots, n\}$ 上の置換全体の作る群を対称群 S_n とよぶのは，つぎのことからである．いまn個の変数 $X_1, X_2, \cdots, X_n$ に関する多項式 $f(X_1, X_2, \cdots, X_n)$ をとり，対称群 S_n の任意の元aに対して

$$f^a(X_1, X_2, \cdots, X_n)=f(X_{1^a}, X_{2^a}, \cdots, X_{n^a})$$

と定義する．たとえば

$$f(X_1, X_2)=X_1^2+2X_1X_2+X_2, \qquad a=(1\ 2)\in S_2$$

に対して

$$f^a(X_1, X_2)=f(X_{1^a}, X_{2^a})=f(X_2, X_1)=X_2^2+2X_1X_2+X_1$$

とする．このときS_nのすべての元に対して変わらない多項式は，$X_1, X_2, \cdots, X_n$ に関する対称式に限るからである．

対称群 S^Ω の部分群を，Ω 上の**置換群**（permutation group）という．$|\Omega|=n$ のとき，Gを**次数**（degree）nの置換群またはn次の置換群という．

例3. $\Omega=\{1, 2, 3, 4\}$ のとき，$G=\left\{1, \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}\right\}$とか，$G=\left\{1, \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}\right\}$は4次の置換群である．

Ωの異なるr個の文字 $i_1, i_2, \cdots, i_r$ に対して，記号 $(i_1\ i_2\ \cdots\ i_r)$ は置換 $x=\begin{pmatrix}i_1 & i_2 & \cdots & i_r & i_{r+1} & i_{r+2} & \cdots & i_n\\ i_2 & i_3 & \cdots & i_1 & i_{r+1} & i_{r+2} & \cdots & i_n\end{pmatrix}$を示すものとする．すなわち置換 $x=(i_1\ i_2\ \cdots\ i_r)$ は $\{i_1, i_2, \cdots, i_r\}$ 上 $i_1^x=i_2, i_2^x=i_3, \cdots, i_r^x=i_1$ であり，残りの文字 $i_{r+1}, i_{r+2}, \cdots, i_n$ に対してはこれらを動かさない置換である．このように書かれた置換 $(i_1\ i_2\ \cdots\ i_r)$ を，長さrの**巡回置換**（cycle）または **r-巡回置換**（r-cycle）という．特に2-巡回置換を**互換**（transposition）という．$r=1$のとき，すなわち $x=(i_1)$ は i_1 を動かさないし，残りの文字も動かさないか

ら単位元である．また $(i_1\ i_2\ \cdots\ i_r)(j_1\ j_2\ \cdots\ j_s)$ は2つの置換 $(i_1\ i_2\ \cdots\ i_r)$ と $(j_1\ j_2\ \cdots\ j_s)$ の積である．

例4. $\Omega=\{1,2,3,4,5,6\}$ 上の置換 $\begin{pmatrix}1&2&3&4&5&6\\2&3&1&4&5&6\end{pmatrix}=(1\ \ 2\ \ 3)$ である．

注 1.1 巡回置換の定義より，つぎのことが成り立つ．

（1） $(i_1\ i_2\ \cdots\ i_r)=(i_2\ i_3\ \cdots\ i_r\ i_1)$.

（2） 任意の $i\in\Omega$ に対して

$$(i_1\ i_2\ \cdots\ i_r)=(i)(i_1\ i_2\ \cdots\ i_r)=(i_1\ i_2\ \cdots\ i_r)(i)$$

である．

（3） 2つの巡回置換 $x=(i_1\ i_2\ \cdots\ i_r)$，$y=(j_1\ j_2\ \cdots\ j_s)$ に対して $\{i_1, i_2, \cdots, i_r\}\cap\{j_1, j_2, \cdots, j_s\}=\phi$ であれば（ϕ は空集合を意味する）

$$xy=(i_1\ i_2\ \cdots\ i_r)(j_1\ j_2\ \cdots\ j_s)=(j_1\ j_2\ \cdots\ j_s)(i_1\ i_2\ \cdots\ i_r)=yx$$

である．

定理 1.2 Ω 上の任意の置換は，互いに共通な文字を含まない巡回置換の積で書ける．このとき積に現れる各巡回置換は，一意的に決まる．

［**証明**］ 置換 x が動かさない文字を $i_1, i_2, \cdots, i_r$ とする．x は $\{i_1, i_2, \cdots, i_r\}$ 上 $(i_1)(i_2)\cdots(i_r)$ である．つぎに，$\Omega-\{i_1, i_2, \cdots, i_r\}\neq\phi$ のとき，任意の文字 $j_1\in\Omega-\{i_1, i_2, \cdots, i_r\}$ をとる．置換 x により $j_1{}^x=j_2$, $j_2{}^x=j_3, \cdots, j_{s-1}{}^x=j_s$ で $j_1, j_2, \cdots, j_s$ はすべて異なり，$j_s{}^x\in\{j_1, j_2, \cdots, j_s\}$ とする．いま $j_s{}^x=j_u$ で $u\neq 1$ とすると，$j_u=j_{u-1}{}^x$ より $j_s=j_{u-1}$ となり，$j_1, j_2, \cdots, j_s$ がすべて異なることに矛盾する．したがって $u=1$，すなわち $j_s{}^x=j_1$ である．これより x は $\{j_1, j_2, \cdots, j_s\}$ 上 $(j_1\ j_2\ \cdots\ j_s)$ である．

つぎに，$\Omega-\{i_1, i_2, \cdots, i_r, j_1, j_2, \cdots, j_s\}\neq\phi$ であれば，k_1 をとり同様にして巡回置換 $(k_1\ k_2\ \cdots\ k_t)$ をうる．以下同じ操作を続けて，つぎの式がえられる．

$$x=(i_1)(i_2)\cdots(i_r)(j_1\ j_2\ \cdots\ j_s)(k_1\ k_2\ \cdots\ k_t)\cdots(l_1\ l_2\ \cdots\ l_u).$$

作り方より各巡回置換は共通な文字を含まず，かつ x により一意的に決まる．□

定理 1.2により，任意の置換 x は互いに共通な文字を含まない巡回置換の積で表すことができる．これを x の**巡回表示**といい，巡回表示に現れる巡回置換を x の**巡回成分**という．置換の巡回表示において，長さ1の巡回成分は注 1.1（2）で示したように書いても書かなくても置換は変わらない．した

がって巡回表示において長さ1の巡回成分を書かない場合が多い．

例 5. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix} = (1\ 2\ 3)(4\ 5)(6) = (1\ 2\ 3)(4\ 5)$

置換 $x(\neq 1)$ を巡回表示したとき，長さ1の巡回成分がいくつかと長さが $r_1, r_2, \cdots, r_k$ の巡回成分よりなるとする．ここで $r_1 \geqq r_2 \geqq \cdots \geqq r_k \geqq 2$ とする．このとき x を $(r_1, r_2, \cdots, r_k)$ **型の置換**という．また単位元の型は（1）とする．

定理 1.3 置換 x の位数は，x の各巡回成分の長さの最小公倍数である．

［**証明**］ x の巡回表示を

$$x = (i_1\ i_2\ \cdots\ i_r)(j_1\ j_2\ \cdots\ j_s)\cdots$$

とすると，注 1.1（3）より

$$x^m = (i_1\ i_2\ \cdots\ i_r)^m(j_1\ j_2\ \cdots\ j_s)^m\cdots$$

である．ここで長さ t の巡回置換の位数は t であるから，x の位数は各巡回成分の長さの最小公倍数である．□

問 1.1 $\{1, 2, 3, 4\}$ 上の対称群 S_4 の部分群をすべてあげよ．

問 1.2 $a_1 = (1\ 2)$, $b_1 = (3\ 4)$, $a_2 = (1\ 2)(3\ 4)$, $b_2 = (1\ 3)(2\ 4)$ とする．このとき $G_1 = \langle a_1, b_1\rangle$, $G_2 = \langle a_2, b_2\rangle$ は位数4の同型な群になることを示せ（この群は4元群である）．

問 1.3 G を $\{1, 2, 3, 4, 5\}$ の上の対称群 S_5 とする．このとき G の元を巡回表示の型に分類し，各型に属する G の元の個数を求めよ．

問 1.4 $a = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$, $b = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$ とするとき，$G = \langle a, b\rangle$ のすべての元を置換の形で示し，かつ G の位数は8であることを示せ（G を **4 元数群** (quaternion group) という）．

§2. 軌　道

G を Ω 上の置換群とする．$i, j \in \Omega$ に対して $i^a = j$ となる G の元 a が存在するとき，i と j は同値であると定義すると，つぎのように同値律が成り立つ．

（1） 反射律： G の単位元1により $i^1 = i$.

（2） 対称律： G の元 a により $i^a = j \Rightarrow G$ の元 a^{-1} により $j^{a^{-1}} = i$.

（3） 推移律： G の元 a, b により $i^a = j,\ j^b = k \Rightarrow G$ の元 ab によ

り $i^{ab}=j$.

したがってこの同値関係により，Ωは同値類 $\Delta_1, \Delta_2, \cdots, \Delta_m$ に類別される．このとき各 Δ_i をGの**軌道** (orbit)，**G-軌道**，またはGの**可移域**という．また $|\Delta_i|$ をΔ_i の長さという．

注 2.1 $i\in\Omega$ に対して $i^G=\{i^x|x\in G\}$とおくと，i^G は i を含むG-軌道である．逆にΔを1つのG-軌道とするとき，任意の $i\in\Delta$ により $\Delta=i^G$ である．

例 1. $\Omega=\{1,2,\cdots,8\}$，$G=\{1,(1\ 2)(3\ 4)(5\ 6)(7\ 8),(1\ 3)(2\ 4)(5\ 7)(6\ 8),(1\ 4)(2\ 3)(5\ 8)(6\ 7)\}$ とするとき，Ω 上の G-軌道は $\{1,2,3,4\}$と$\{5,6,7,8\}$ である．

Ω上の置換群GがΩ上 **t 重可移** (t-transitive) であるとは，$|\Omega|\geqq t$ で，Ωの t 個の異なる文字からなる任意の2つの順列 $(i_1, i_2, \cdots, i_t)$，$(j_1, j_2, \cdots, j_t)$ に対してGに$\begin{pmatrix} i_1 & i_2 & \cdots & i_t & \cdots \\ j_1 & j_2 & \cdots & j_t & \cdots \end{pmatrix}$なる元が存在するときをいい，このとき G を Ω 上の **t 重可移群** という．ここで $t=1$ のとき，GはΩ上 **可移** であるまたはΩ上の **可移群** (transitive group)，$t\geqq 2$ のとき，Gを **多重可移群** (multiply transitive group) という．GがΩ上可移であることは，ΩがGの1つの軌道であることにほかならない．また定義より

注 2.2 t 重可移群 ($t\geqq 2$) は $(t-1)$ 重可移群である．

定理 2.3 Ω上の置換群GがΩ上 t 重可移であるためには，任意の t 個の異なる文字からなる順列 $(i_1, i_2, \cdots, i_t)$ に対して，Gに$\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ i_1 & i_2 & \cdots & i_t & \cdots \end{pmatrix}$なる元が存在すればよい．

［**証明**］ t 個の異なる文字からなる任意の2つの順列 $(i_1, i_2, \cdots, i_t)$，$(j_1, j_2, \cdots, j_t)$ に対して仮定よりGに

$$x=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ i_1 & i_2 & \cdots & i_t & \cdots \end{pmatrix}, \qquad y=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ j_1 & j_2 & \cdots & j_t & \cdots \end{pmatrix}$$

なる元が存在する．このとき

$$x^{-1}y=\begin{pmatrix} i_1 & i_2 & \cdots & i_t & \cdots \\ 1 & 2 & \cdots & t & \cdots \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ j_1 & j_2 & \cdots & j_t & \cdots \end{pmatrix}=\begin{pmatrix} i_1 & i_2 & \cdots & i_t & \cdots \\ j_1 & j_2 & \cdots & j_t & \cdots \end{pmatrix}\in G$$

となりGはΩ上t重可移である． □

多重可移群の例としては次節で述べる対称群がある．

問 2.1 $\{1,2,3,4\}$ 上の2重可移群をあげよ．

問 2.2 G_1, G_2 を群として同型であるΩ上の置換群とする．いまG_1がΩ上可移であれば，G_2 もΩ上可移であるといえるか．

問 2.3 前節問1.4の $\Omega=\{1,2,\cdots,8\}$ 上の置換群 $G=\langle a,b\rangle$

$$a=(1\ 2\ 3\ 4)(5\ 6\ 7\ 8),$$

$$b=(1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$$

は Ω 上可移であるが，2重可移にならないことを示せ．

問 2.4 Vを標数が2と異なる $GF(q)$ 上の2次元ベクトル空間，G をつぎのV上の置換の作る置換群とする．

$$a_\alpha\ ;\quad (\lambda_1,\lambda_2)^{a_\alpha}=(\alpha\lambda_1,\alpha^{-1}\lambda_2)$$

$$b_\alpha\ ;\quad (\lambda_1,\lambda_2)^{b_\alpha}=(\alpha\lambda_1,-\alpha^{-1}\lambda_2)$$

$$c\ ;\quad (\lambda_1,\lambda_2)^{c}=(\lambda_2,\lambda_1),\qquad (\lambda_1,\lambda_2)\in V,\ \alpha\in GF(q)-\{0\}.$$

このとき，Gの位数とV上のG-軌道の長さを求めよ．

§3. 対称群，交代群

補題 3.1 x, y をΩ上の置換とする．いま

$$x=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}=(j_1\ j_2\ \cdots\ j_r)(k_1\ k_2\ \cdots\ k_s)\cdots$$

とすると

$$x^y=\begin{pmatrix}1^y & 2^y & \cdots & n^y\\ i_1{}^y & i_2{}^y & \cdots & i_n{}^y\end{pmatrix}=(j_1{}^y\ j_2{}^y\ \cdots\ j_r{}^y)(k_1{}^y\ k_2{}^y\ \cdots\ k_s{}^y)\cdots$$

である．

［証明］ 任意の $i\in\Omega$ に対して

$$(i^y)^{x^y}=(i^y)^{y^{-1}xy}=i^{xy}=(i^x)^y$$

であるから，x^y は i^y を $(i^x)^y$ にうつす．したがって $x=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$ とすると $x^y=\begin{pmatrix}1^y & 2^y & \cdots & n^y\\ i_1{}^y & i_2{}^y & \cdots & i_n{}^y\end{pmatrix}$ である．また $x=(j_1\ j_2\ \cdots\ j_r)(k_1\ k_2\ \cdots\ k_s)\cdots$ とすると

$$x^y=((j_1\ j_2\ \cdots\ j_r)(k_1\ k_2\ \cdots\ k_s)\cdots)^y=(j_1\ j_2\ \cdots\ j_r)^y(k_1\ k_2\ \cdots\ k_s)^y\cdots$$

であり，上で示したように $(j_1\ j_2\ \cdots\ j_r)^y=(j_1{}^y\ j_2{}^y\ \cdots\ j_r{}^y)$，$(k_1\ k_2\ \cdots\ k_s)^y=(k_1{}^y\ k_2{}^y$

$\cdots k_s{}^y), \cdots$ であるから，$x^y=(j_1{}^y\ j_2{}^y\ \cdots\ j_r{}^y)(k_1{}^y\ k_2{}^y\ \cdots\ k_s{}^y)\cdots$ である．□

この補題において $x=(j_1\ j_2\ \cdots\ j_r)(k_1\ k_2\ \cdots\ k_s)\cdots$ は，x を巡回置換の積で表したもので，巡回表示である必要はない．

定理 3.2 対称群 S_n の元 x, y が S_n で共役であるための必要十分な条件は，x と y の巡回表示の型が一致することである．

［証明］（必要条件） x と y が S_n で共役であるとする．すなわち $x^a=y$ となる $a\in S_n$ が存在するとする．いま x の巡回表示を $x=(i_1\ i_2\ \cdots\ i_r)(j_1\ j_2\ \cdots\ j_s)\cdots$ とすると，補題 3.1 より $y=x^a=(i_1{}^a\ i_2{}^a\ \cdots\ i_r{}^a)(j_1{}^a\ j_2{}^a\ \cdots\ j_s{}^a)\cdots$ となり，これは y の巡回表示である．したがって x と y の巡回表示の型は一致する．

（十分条件） x と y の巡回表示の型が一致するとする．

$$x=(i_1\ i_2\ \cdots\ i_r)(j_1\ j_2\ \cdots\ j_s)\cdots$$
$$y=(i'_1\ i'_2\ \cdots\ i'_r)(j'_1\ j'_2\ \cdots\ j'_s)\cdots$$

を x と y の巡回表示とし，ともに巡回成分を長いものから順次並べたものとする．このとき $a=\begin{pmatrix} i_1 & i_2 & \cdots & i_r & j_1 & j_2 & \cdots & j_s & \cdots \\ i'_1 & i'_2 & \cdots & i'_r & j'_1 & j'_2 & \cdots & j'_s & \cdots \end{pmatrix}\in S_n$ が存在して，補題3.1により $x^a=y$ である．□

例 1. 対称群 S_5 において共役類は 7 個存在し，その代表元はつぎの 1，(1 2)，(1 2)(3 4)，(1 2 3)，(1 2 3 4)，(1 2 3 4 5)，(1 2)(3 4 5) である．

補題 3.3 任意の置換は互換の積で書ける（この積は巡回表示の意味ではない）．

［証明］ $(i_1\ i_2\ \cdots\ i_r)=(i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_r)$ である．□

定理 3.4 置換を互換の積で表すとき，それに現れる互換の数は一定ではないが，偶数個であるか奇数個であるかは定まっている．

［証明］ (1 2)＝(1 2)(1 2)(1 2) のように互換の積で表す方法は幾通りでもある．

いま置換 x を互換の積で表したとき，その互換の個数が偶数個の場合と奇数個の場合があるとする．x^{-1} は x の互換の並びかたの順序をちょうど反対にしたものであるから，x としては偶数個の互換の積を，x^{-1} としては奇数個の互換の積をとる．すると単位元 $1=xx^{-1}$ は奇数個の互換の積となる．したがって単位元は奇数個の互換の積で書けないことを示せばよい．いまこのことを互換の個数に関する帰納法で証明する．

単位元1は1個の互換 $(i\ j)$ に等しくない．

いま単位元1が奇数 r 個の互換の積 $1=(i_1\ j_1)(i_2\ j_2)\cdots(i_r\ j_r)$ と書け，奇数 $r-2$ 個の互換の積では書けないとする．文字 i_1 に注目する．$(i_1\ j_1)(i_2\ j_2)$ について

$\{i_1, j_1\}=\{i_2, j_2\}$ ならば，$(i_1\ j_1)(i_2\ j_2)=1$ となりこの2つの互換をとり除くことにより，単位元が $r-2$ 個の互換の積となり仮定に反する．

$\{i_1, j_1\}\cap\{i_2, j_2\}=\{i_1\}$ ならば，$i_2=i_1$，$j_1\neq j_2$ としてよい．

このとき

$$(i_1\ j_1)(i_2\ j_2)=(i_1\ j_1\ j_2)=(j_1\ j_2)(i_1\ j_1)$$

となる．

$\{i_1, j_1\}\cap\{i_2, j_2\}=\{j_1\}$ ならば，$j_1=j_2$，$i_1\neq i_2$ としてよい．このとき

$$(i_1\ j_1)(i_2\ j_2)=(j_1\ i_1\ i_2)=(i_2\ j_1)(i_1\ i_2)$$

となる．

$\{i_1, j_1\}\cap\{i_2, j_2\}=\phi$ ならば

$$(i_1\ j_1)(i_2\ j_2)=(i_2\ j_2)(i_1\ j_1)$$

となる．

以上の操作により i_1 が現れる互換を順次うしろに送ることができ，これにより互換の個数は変わらないが，i_1 を含む互換は最後の互換のみとなる．このとき i_1 は単位元で動かされることになり矛盾である．したがって単位元は奇数個の互換の積で書けない．すなわち任意の置換を互換の積で表すとき，その個数が偶数か奇数かは一定である．□

置換を互換の積で表したとき，その個数が偶数個のときを**偶置換** (even permutation)，奇数個のときを**奇置換** (odd permutation) という．

また，長さ r の巡回置換は $(i_1\ i_2\ \cdots\ i_r)=(i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_r)$ であるから，$r-1$ 個の互換の積で書ける．したがって

注 3.5 長さ r の巡回置換は，r が偶数のとき奇置換，奇数のとき偶置換である．

定理 3.6 G を置換群，H を偶置換全体からなる G の部分集合とする．もし G が奇置換を含むならば，H は G における指数2の正規部分群である．

［**証明**］ 2つの偶置換の積は偶置換であるから，定理 1；1.3 より G の偶置換全体からなる集合 H は G の部分群である．

G が奇置換を含むとする．いま x, y を G の任意の奇置換とすると，xy^{-1} は偶置換と

なりHの元で，したがってxとyはHを法とするGの同じ剰余類に属する．これより

$$G = H + Hx, \qquad |G : H| = 2$$

となる．ここで指数２の部分群は定理 1；2.2 より正規部分群であるから，HはGの正規部分群である．□

対称群 S^{Ω}（または S_n）の偶置換全体の集合は定理 3.6 より対称群の指数２の正規部分群になる．これを**交代群** (alternating group) といい A^{Ω} または A_n と書く．

定理 3.7 $|S_n| = n!$, $|A_n| = n!/2$.

［証明］ S_n の元を$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$と書くと，この表し方の下の段 $(i_1, i_2, \cdots, i_n)$ はn個の文字 1, 2, ⋯, n の順列である．逆に任意の順列 $(i_1, i_2, \cdots, i_n)$ により S_n の元$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$が一意的に決まる．したがって S_n の位数はn個の文字の順列の個数 $n!$ に等しい．

また $|S_n : A_n| = 2$ より，$|A_n| = n!/2$ である．□

この定理より，Gをn次の置換群とすると，Gは対称群 S_n の部分群であるから，Gの位数 は S_n の位数 $n!$ の約数であることがわかる．

定理 3.8 aを交代群 A_n の元，Cをaを含む対称群 S_n の共役類とする．このとき $C \subset A_n$ で

（１） aと可換な奇置換が存在するとき，そのときに限りCはまた A_n の共役類である．

（２） Cが A_n の共役類でないとき，A_n においてCは同数個の元を含む２つの共役類にわかれる．

［証明］ A_n は S_n の正規部分群であるから，aを含む S_n の共役類Cは A_n に含まれる．

uを S_n の任意の奇置換とすると，$S_n = A_n + uA_n$ である．いまaを含む A_n の共役類を C', a^u を含む A_n の共役類を C'' とする．このとき

$$C = \{a^x \mid x \in S_n\} = \{a^x \mid x \in A_n\} \cup \{a^{ux} \mid x \in A_n\} = C' \cup C'' \qquad ①$$

である．

（1） a と可換な奇置換が存在するとする．このときuとしてaと可換な奇置換をとってよい．すると $a^u = a$ となり，①より $C'' = C'$ である．すなわち $C = C'$ でCは

aを含む A_n の共役類である．

逆に C はaを含む A_n の共役類であるとする．すると $C=C'$ で，①より $C''\subseteqq C=C'$ である．ここで C', C'' は共に A_n の共役類であるから $C'=C''$ である．したがって $a\in C''$ となり，$a=a^{ux}$ となる $x\in A_n$ が存在する．ここで ux は奇置換であるから，a と可換な奇置換が存在する．

（2） Cが A_n の共役類でないとする．①よりCは A_n の２つの共役類 C', C'' の和集合である．$A_n \trianglelefteq S_n$ より $uA_n=A_nu$ である．したがって

$$C''=\{a^{ux}\,|\,x\in A_n\}=\{a^{xu}\,|\,x\in A_n\}=C'^u$$

となり，$|C'|=|C''|$ である．□

例 2. 交代群 A_5 において共役類は５個存在し，その代表元は 1，(1 2)(3 4)，(1 2 3)，(1 2 3 4 5)，(1 2 3 5 4) である．

定 理 3.9 $|\Omega|=n$ とする．

（1） Ω上の対称群 S_n はΩの上でn重可移である．

（2） Ω上の交代群 A_n はΩの上でちょうど $(n-2)$ 重可移である．

［証 明］（1） Ωの文字の任意の順列 $(i_1, i_2, \cdots, i_n)$ に対して，S_n は$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$なる元をもつ．したがって定理 2.3 より S_n はΩ上n重可移である．

（2） Ωの異なる $n-2$ 個の文字からなる任意の順列 $(i_1, i_2, \cdots, i_{n-2})$ に対して，残りのΩの２個の文字を i_{n-1}, i_n とする．このとき$\begin{pmatrix}1 & 2 & \cdots & n-2 & n-1 & n\\ i_1 & i_2 & \cdots & i_{n-2} & * & *\end{pmatrix}$なる置換は

$$x=\begin{pmatrix}1 & 2 & \cdots & n-2 & n-1 & n\\ i_1 & i_2 & \cdots & i_{n-2} & i_{n-1} & i_n\end{pmatrix}$$

または

$$y=\begin{pmatrix}1 & 2 & \cdots & n-2 & n-1 & n\\ i_1 & i_2 & \cdots & i_{n-2} & i_n & i_{n-1}\end{pmatrix}$$

のいずれかで，$y=x\cdot(i_{n-1}\ i_n)$ である．したがって x か y は偶置換になり A_n の元で，定理 2.3 より A_n は Ω 上 $(n-2)$ 重可移である．

一方 $n-1$ 個の文字からなる順列 $(1, 2, \cdots, n-1)$ をとると，順列 $(i_1, i_2, \cdots, i_{n-2}, i_{n-1})$ に対して$\begin{pmatrix}1 & 2 & \cdots & n-2 & n-1 & n\\ i_1 & i_2 & \cdots & i_{n-2} & i_{n-1} & *\end{pmatrix}$なる置換は$x$のみであり，順列 $(i_1, i_2, \cdots, i_{n-2}, i_n)$ に対して$\begin{pmatrix}1 & 2 & \cdots & n-2 & n-1 & n\\ i_1 & i_2 & \cdots & i_{n-2} & i_n & *\end{pmatrix}$なる置換は y のみである．上で示したようにxかyのいずれかは奇置換で A_n の元ではない．よって A_n は $(n-1)$ 重可移にはなりえない（なお，$(n-1)$ 重可移であればn重可移になることからもいえる）．□

補 題 3.10 （1） 交代群 $A_n=\langle (i\ j\ k)\,|\,i, j, k(\neq)\in\Omega\rangle$ $(n\geqq 3)$ で

ある．

（2） $n \geqq 5$ のとき，交代群 $A_n = \langle (i\ j)(k\ l) \mid i, j, k, l (\neq) \in \Omega \rangle$ である．

［証明］（1） 注3.5より $(i\ j\ k)$ は偶置換であるから A_n の元である．

逆は，A_n の任意の元は偶数個の互換の積で書けるから，2つの互換の積 $(i\ j)(k\ l)$ $(\{i, j\} \neq \{k, l\})$ が3－巡回置換の積であることを示せばよい．

$\{i, j\}$ と $\{k, l\}$ が共通の文字を1つもつとき，$i = k$，$j \neq l$ としてよい．このとき $(i\ j)(k\ l) = (i\ j\ l)$ である．また $\{i, j\}$ と $\{k, l\}$ が共通の文字をもたないとき

$$(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ k\ j)(j\ l\ k)$$

である．したがって，$A_n = \langle (i\ j\ k) \mid i, j, k (\neq) \in \Omega \rangle$ である．

（2） $(i\ j\ k)$ を A_n の任意の3－巡回置換とする．$n \geqq 5$ より $l, l' (\neq) \in \Omega - \{i, j, k\}$ をとると

$$(i\ j\ k) = (i\ j)(i\ k) = (i\ j)(l\ l')(l\ l')(i\ k)$$

である．ここで $(i\ j)(l\ l')$，$(l\ l')(i\ k)$ は共に $(2, 2)$ 型の巡回表示であるから $(i\ j\ k) \in \langle (i_1\ i_2)(i_3\ i_4) \mid i_1, i_2, i_3, i_4 (\neq) \in \Omega \rangle$ となり（1）より成り立つ．□

補題 3.11（1） $n \neq 2, 4$ のとき，対称群 S_n の $S_n, 1$ と異なる正規部分群は交代群 A_n のみである．

（2） 対称群 S_4 の $S_4, 1$ と異なる正規部分群は，交代群 A_4 と4元群 $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ である．

［証明］ $n \geqq 3$ とし N を S_n, 1 と異なる S_n の正規部分群とする．$n = 3$ のとき $N = A_3$ であることは位数より明らかである．したがって以下 $n \geqq 4$ とする．

N の元 $a (\neq 1)$ をとり，a の巡回表示を $a = (i\ j\ \cdots)\cdots$ とする．$k \in \Omega - \{i, j\}$ をとり互換 $u = (i\ k)$ を作る．$N \triangleleft S_n$ より $a^{-1}a^u \in N$ である．一方補題3.1を用いて

$$a^{-1}a^u = a^{-1}u^{-1}au = (u^{-1})^a u = (j\ k^a)(i\ k)$$

である．このとき

（i） $k^a = i$ または k であれば，$(j\ k^a)(i\ k) = (i\ j\ k)$ または $(k\ j\ i)$ である．

（ii） $k^a \neq i, j$ であれば，$(j\ k^a)(i\ k)$ は $(2, 2)$ 型の置換である．

定理3.2より $C_1 = \{(i\ j\ k) \mid i, j, k (\neq) \Omega\}$ および $C_2 = \{(i\ j)(k\ l) \mid i, j, k, l (\neq) \in \Omega\}$ は共に S_n の共役類である．ここで $a^{-1}a^u \in N \triangleleft S_n$ であるから（i）または（ii）が成り立つとき，それぞれ $C_1 \subset N$ または $C_2 \subset N$ である．したがって $n \geqq 5$ のとき補題3.10より $N = A_n$ である．

$n=4$ とする．(i) のとき補題 3.10 (1) より $N=A_4$ である．(ii) が成り立つとする．いまNが奇置換を含むとする．$N \triangleleft S_4$ で S_4 の奇置換は互換か 4-巡回置換であるから，定理 3.2 よりNはすべての互換または 4-巡回置換を含む．このとき明らかに $N=S_4$ となり仮定に反する．したがってNは偶置換のみを含み，$N \leqq A_4$ である．$N \neq A_4$ とすると $C_2 \subset N$ より $3=|C_2|<|N|$ となり，$|A_4|=4 \cdot 3$ であるから $N=\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ である．□

定理 3.12　$n \geqq 5$ のとき交代群 A_n は単純群である．

[証明]　Nを1と異なる A_n の正規部分群とし，$N=A_n$ を示す．Nが 3-巡回置換 $(i\ j\ k)$ を含むとする．$n \geqq 5$ より $l, l' (\neq) \in \Omega - \{i, j, k\}$ をとると互換 $(l\ l')$ は $(i\ j\ k)$ と可換である．したがって定理 3.8 (1) よりすべての3-巡回置換は $(i\ j\ k)$ と A_n で共役である．ここで $(i\ j\ k) \in N \trianglelefteq A_n$ であるから，Nはすべての 3-巡回置換を含み，補題 3.10 (1) より $N=A_n$ である．

Nが (2,2) 型の置換 $(i\ j)(k\ l)$ を含むとする．互換 $(i\ j)$ は $(i\ j)(k\ l)$ と可換であるから，定理 3.8 (1) および補題 3.10 (2) より上の場合と同じようにして $N=A_n$ となる．したがってNは 3-巡回置換または (2, 2) 型の置換を含むことを示せばよい．いまaを1と異なるNの元とする．

(i)　aが長さ5以上の巡回成分を含むとし，aの巡回表示を $a=(i\ j\ k\ l\ m\ \cdots)\cdots$ とする．$u=(j\ k\ l) \in A_n$ をとると $a^u a^{-1} \in N$ である．一方

$$a^u a^{-1} = u^{-1}aua^{-1} = u^{-1}u^{a^{-1}} = (j\ l\ k)(i\ j\ k) = (i\ j\ l)$$

であるから，Nは 3-巡回置換をもつ．

(ii)　aが長さ2または4の巡回成分をもつとする．aの位数は $2^r \cdot m$, $r \geqq 1$, $(2, m)=1$ ($(2, m)$ は2とmの最大公約数) である．$b=a^{2^{r-1} \cdot m}$ とおくとbは位数2のNの元である．bが (2, 2) 型の置換でないならば，bは偶置換だから巡回表示は

$$b=(i\ j)(k\ l)(i'\ j')(k'\ l')\ \cdots$$

である．$u=(i\ j\ i') \in A_n$ をとると

$$b^u b^{-1} = u^{-1}u^{b^{-1}} = (i\ i'\ j)(j\ i\ j') = (i\ i')(j\ j') \in N$$

となり，Nは (2,2) 型置換をもつ．

(iii)　以上よりaの巡回成分の長さがすべて3のときを考えればよい．aが 3-巡回置換でないならば，aの巡回表示は

$$a=(i\ j\ k)(i'\ j'\ k')\cdots$$

である．$u=(i\ j\ i') \in A_n$ をとると

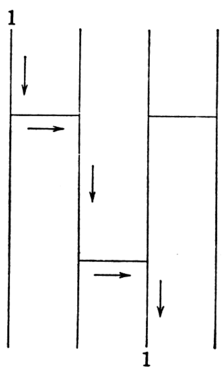
$$a^u a^{-1} = u^{-1} u^{a^{-1}} = (i\ i'\ j)(k\ i\ k') = (i\ i'\ j\ k'\ k) \in N$$

となり，（i）よりNは3-巡回置換をもつ．

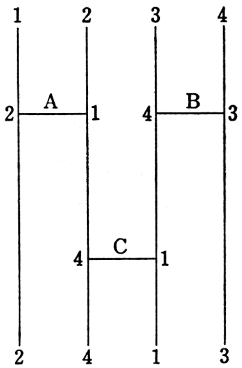
以上より $N = A_n$ となり，A_n $(n \geqq 5)$ は単純群である．□

あみだくじと置換

一般によく使われているあみだくじと置換との関係について述べる．あみだくじは2–1図のようにいくつかの縦線と，縦線を結ぶいくつかの横線からできているくじで，縦線にそって下に降りてゆくが，横線と交わると横線上を横に進み，つぎの縦線をまた降りるものとする．たとえば2–1図で上の1は矢印のように下の1にゆきつくものとする．



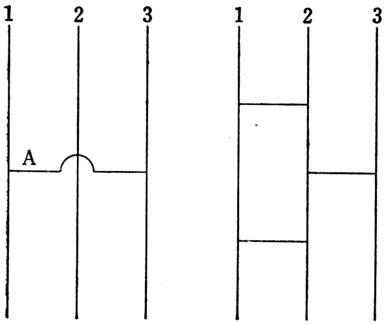
2-1 図



2-2 図

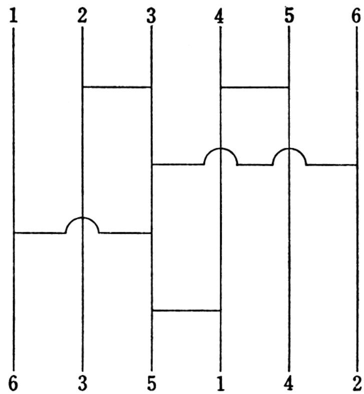
いまこのあみだくじの出発点に2–2図のように 1,2,3,4 と番号をうつと，それぞれ下の 1,2,3,4 のところにゆく．これよりこのあみだくじは順列 (1, 2, 3, 4) を順列 (2, 4, 1, 3) にうつすものと考えられる．したがってこのあみだくじは置換$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$と同じはたらきをしている．一般に$n$本の縦線からなるあみだくじは$n$個の文字の上の置換をおこなうとみなすことができる．

また横線は互換と同じはたらきをする．たとえば2–2図の横線Aは互換(1 2)，横線Bは互換 (3 4)，横線Cは互換 (1 4) であり，このあみだくじはまた$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2)(3\ 4)(1\ 4)$と置換は互換の積で書けることも示している．



(a)　　(b)

2-3 図



2-4 図

逆に任意の置換は互換の積で書けるから，この置換と同じはたらきをするあみだくじを作ることができる．ここで互換と横線がうまく対応するように，2-3 図 (a) のような新しい横線を用いる．図 (a) で横線 A は縦線 2 と交わらないとする．したがって横線 A は縦線 1 と 3 を結んだものである（これは図 (b) のあみだくじと同じである）．この方法を用いて 置換 (2 3)(4 5)(2 6)・(1 6)(1 5) $=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ と同じはたらきをするあみだくじを 2-4 図のように作ることができる．

問 3.1 対称群 $S_n=\langle(1\ 2), (1\ 3), \cdots, (1\ n)\rangle$ を示せ．

問 3.2 対称群 $S_n=\langle(1\ 2), (2\ 3\ \cdots\ n)\rangle$ を示せ．

問 3.3 a を交代群 A_n の元，C を a を含む対称群 S_n の共役類とする．a が長さ偶数の巡回成分をもつか，奇数の同じ長さの巡回成分を 2 個以上もつとき，そのときに限り C は A_n の共役類になることを示せ．

問 3.4 次数 n の t 重可移群 G $(t \geqq 3)$ が $2t-3$ 個以下の文字を動かし，残りの文字を固定する元 $(\neq 1)$ を含むならば，G は交代群 A_n を含むことを示せ．

§4. 安定化群

G を Ω 上の置換群，Δ を Ω の部分集合とするとき，$G_\Delta=\{x \in G \mid i^x=i(\forall i \in \Delta)\}$ を G における Δ の（点ごとの）**安定化群** (stabilizer) という．特に $\Delta=\{i, j, \cdots, m\}$ のとき，G_Δ を $G_{ij\cdots m}$ とも書く．また $G_{(\Delta)}=\{x \in G \mid \Delta^x=\Delta\}$

をGにおけるΔの集合としての安定化群という．特に$\Delta=\{i, j, \cdots, m\}$のとき$G_{(\Delta)}$を$G_{(i,j,\cdots,m)}$とも書く．このとき，つぎのことは明らかである．

注 4.1 G_Δ, $G_{(\Delta)}$は共にGの部分群である．

例 1. Gを$\Omega=\{1,2,3,4,5\}$上の対称群S_5とし$\Delta=\{1,2\}$とする．このとき

$$G_\Delta=G_{1\,2}=\langle(3\ 4\ 5),(4\ 5)\rangle\cong S_3$$

$$G_{(\Delta)}=G_{(1,2)}=\langle(1\ 2),G_{1\,2}\rangle$$

である．

補 題 4.2 GをΩ上の置換群，Δ, ΓをΩの部分集合とする．

(1) $G_{\Delta\cup\Gamma}=G_\Delta\cap G_\Gamma=(G_\Delta)_\Gamma$.

(2) HをGの部分群とするとき，$x\in G$に対して

$$(H_\Delta)^x=H^x{}_{\Delta^x},\qquad (H_{(\Delta)})^x=H^x{}_{(\Delta^x)}$$

である．特に

$$(G_\Delta)^x=G_{\Delta^x},\qquad (G_{(\Delta)})^x=G_{(\Delta^x)}$$

である．

(3) $G_\Delta\trianglelefteq G_{(\Delta)}$.

［証 明］ (1) $x\in G_{\Delta\cup\Gamma}\Longleftrightarrow i^x=i,\ \forall i\in\Delta\cup\Gamma\Longleftrightarrow i^x=i,\ j^x=j,\ \forall i\in\Delta,\ \forall j\in\Gamma$

$$\Longleftrightarrow x\in G_\Delta\cap G_\Gamma$$

である．したがって$G_{\Delta\cup\Gamma}=G_\Delta\cap G_\Gamma$となる．また

$$x\in G_\Delta\cap G_\Gamma\Longleftrightarrow x\in G_\Delta,\ j^x=j,\ \forall j\in\Gamma\Longleftrightarrow x\in(G_\Delta)_\Gamma$$

である．したがって$G_\Delta\cap G_\Gamma=(G_\Delta)_\Gamma$となる．

(2) $y\in(H_\Delta)^x\Longleftrightarrow y^{x^{-1}}\in H_\Delta\Longleftrightarrow y^{x^{-1}}\in H,\ i^{xyx^{-1}}=i,\ \forall i\in\Delta$

$$\Longleftrightarrow y\in H^x,\ i^{xy}=i^x,\ \forall i\in\Delta\Longleftrightarrow y\in H^x{}_{\Delta^x}$$

である．したがって$(H_\Delta)^x=H^x{}_{\Delta^x}$となる．

また$(H_{(\Delta)})^x=H^x{}_{(\Delta^x)}$も同じようにして示される．

(3) $G_\Delta\leqq G_{(\Delta)}$は明らかである．任意の$x\in G_{(\Delta)}$に対して，$\Delta^x=\Delta$であるから(2)を用いて，$(G_\Delta)^x=G_{\Delta^x}=G_\Delta$となり，$G_\Delta\trianglelefteq G_{(\Delta)}$である．□

定 理 4.3 GをΩ上の置換群，$i\in\Omega$とする．このとき$a\in G$に対して$G_ia=\{x\in G\,|\,i^x=i^a\}$で，

(1) $\Delta=\{i=i_1, i_2, \cdots, i_m\}$を$i$を含む長さ$m$の$G$-軌道とすると，$i^{x_k}=i_k$となる$x_k\in G$ $(k=1,2,\cdots,m)$が存在して，$G=G_ix_1+G_ix_2+\cdots+G_ix_m$

である．

（2） 逆に $G = G_i x_1 + G_i x_2 + \cdots + G_i x_m$ とすると，$\Delta = \{i^{x_1}, i^{x_2}, \cdots, i^{x_m}\}$ は i を含む長さ m の G-軌道である．

［証 明］ $i^{G_i a} = \{i^a\}$ である．逆に $i^x = i^a$ ならば，$i^{xa^{-1}} = i$，$xa^{-1} \in G_i$ となり $x \in G_i a$ である．したがって，$G_i a = \{x \in G \mid i^x = i^a\}$ である．

（1） $\Delta = \{i = i_1, i_2, \cdots, i_m\}$ を i を含む長さ m の G-軌道とする．このとき G-軌道の定義より，$i^{x_k} = i_k$ である $x_k \in G$ $(k = 1, 2, \cdots, m)$ が存在する．任意の $x \in G$ に対して，Δ は i を含む G-軌道であるから $i^x \in \Delta$，すなわち $i_k \in \Delta$ が存在して $i^x = i_k = i^{x_k}$ である．したがって上で示したことより $x \in G_i x_k$ となり，$G = \bigcup_{k=1}^{m} G_i x_k$ である．

ここで $x_k \neq x_{k'}$ であれば，$G_i x_k = \{x \mid i^x = i^{x_k} = i_k\}$，$G_i x_{k'} = \{x \mid i^x = i^{x_{k'}} = i_{k'}\}$ より $G_i x_k \cap G_i x_{k'} = \phi$ である．すなわち $G = \bigcup_{k=1}^{m} G_i x_k$ は G_i を法とする左分解 $G = G_i x_1 + G_i x_2 + \cdots + G_i x_m$ である．

（2） 逆に $G = G_i x_1 + G_i x_2 + \cdots + G_i x_m$ とする．上で証明したことより $G_i x_k = \{x \mid i^x = i^{x_k}\}$ で，$x_k \neq x_{k'}$ であれば $i^{x_k} \neq i^{x_{k'}}$ であるから，$\Delta = \{i^{x_1}, i^{x_2}, \cdots, i^{x_m}\}$ は i を含む長さ m の G-軌道である．□

系 4.4 $|G| = |G_i| \cdot |i^G|$

［証 明］ i を含む G-軌道は i^G である．したがって定理 4.3（1）より $|G| = |G_i| \cdot |i^G|$ である．□

定 理 4.5 G を Ω 上の置換群，Δ, Γ を G-軌道とし，$(|\Delta|, |\Gamma|) = d$ とする．このとき $i \in \Delta$ に対して，G_i の Γ 上の軌道の長さは $|\Gamma|/d$ の倍数である．

特に $d = 1$ であれば，Γ はまた G_i-軌道である．

［証 明］ $j \in \Gamma$ に対して j を含む G_i-軌道を Γ_j とし，$i \in \Delta$ を含む G_j-軌道を Δ_i とする．系 4.4 を用いて

$$\frac{|G|}{|G_{ij}|} = \frac{|G|}{|G_i|} \cdot \frac{|G_i|}{|G_{ij}|} = |\Delta| \cdot |\Gamma_j|$$

$$= \frac{|G|}{|G_j|} \cdot \frac{|G_j|}{|G_{ij}|} = |\Gamma| \cdot |\Delta_i|$$

である．この式より

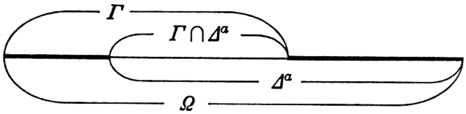
$$|\Gamma_j| = \frac{|\Gamma| \cdot |\Delta_i|}{|\Delta|} = \frac{\frac{|\Gamma|}{d} \cdot |\Delta_i|}{\frac{|\Delta|}{d}}$$

である．一方 $(|\Gamma|, |\Delta|) = d$ であるから $(|\Gamma|/d, |\Delta|/d) = 1$ である．したがって $|\Delta_i|/(|\Delta|/d)$ は整数となり，j を含む G_i- 軌道 Γ_j の長さは $|\Gamma|/d$ の倍数である．

特に $d=1$ であれば $|\Gamma_j|$は$|\Gamma|$ の倍数で，$\Gamma_j \subseteqq \Gamma$ より $\Gamma_j = \Gamma$ となり Γ は G_i-軌道である．□

定理 4.6 GをΩ上の可移群，Δ, Γ をΩの部分集合とする．G_Δ が $\Omega - \Delta$ 上可移，G_Γ が $\Omega - \Gamma$ 上可移で，$|\Gamma| \leqq |\Delta|$とすると，$\Gamma \subseteqq \Delta^a$ したがって $(G_\Delta)^a \leqq G_\Gamma$ となる元 $a \in G$ が存在する．

［証 明］ aがGの元をわたるとき，$|\Gamma \cap \Delta^a|$ を最大にする元をあらためてaとする．$\Gamma \cap \Delta^a = \Gamma$ であれば $\Gamma \subseteqq \Delta^a$ となり，補題 4.2（2）より $(G_\Delta)^a = G_{\Delta^a} \leqq G_\Gamma$ である．したがって $\Gamma \cap \Delta^a \subsetneqq \Gamma$ として矛盾を導く．なおこのとき $\Delta \subsetneqq \Omega$ である．



（i） $\Gamma \cup \Delta^a = \Omega$ とする．このとき

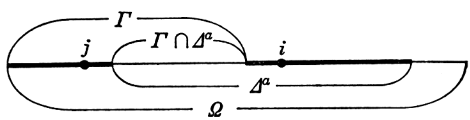
$$|\Omega| = |\Gamma| + |\Delta^a| - |\Gamma \cap \Delta^a| \quad ①$$

である．一方GはΩ上可移であるから，$i \in \Omega - \Delta$, $j \in \Omega - \Gamma$ に対して $j = i^b$ となる $b \in G$ が存在する．$j = i^b \in (\Omega - \Delta)^b = \Omega - \Delta^b$ より $j \in (\Omega - \Gamma) \cap (\Omega - \Delta^b)$ となり，$j \notin \Gamma \cup \Delta^b$ である．したがって

$$|\Omega| \gneqq |\Gamma \cup \Delta^b| = |\Gamma| + |\Delta^b| - |\Gamma \cap \Delta^b| \quad ②$$

である．①と②より $|\Gamma| + |\Delta^a| - |\Gamma \cap \Delta^a| \gneqq |\Gamma| + |\Delta^b| - |\Gamma \cap \Delta^b|$ で $|\Delta^a| = |\Delta^b|$ であるから $|\Gamma \cap \Delta^b| \gneqq |\Gamma \cap \Delta^a|$ となり，$|\Gamma \cap \Delta^a|$ が最大であることに反する．

（ii） $\Gamma \cup \Delta^a \subsetneqq \Omega$ とする．このとき $(\Omega - \Gamma) \cap (\Omega - \Delta^a) \neq \phi$ で，仮定より G_Γ は $\Omega - \Gamma$ 上可移，



G_{Δ^a} は $\Omega - \Delta^a$ 上可移であるから，$\langle G_\Gamma, G_{\Delta^a} \rangle$ は $(\Omega - \Gamma) \cup (\Omega - \Delta^a) = \Omega - (\Gamma \cap \Delta^a)$ 上可移である．したがって $i \in \Delta^a - (\Gamma \cap \Delta^a), j \in \Gamma - (\Gamma \cap \Delta^a)$ に対して $i^b = j$ である $b \in \langle G_\Gamma, G_{\Delta^a} \rangle$が存在する．このとき $\Delta^{ab} \supseteqq ((\Delta^a \cap \Gamma) \cup \{i\})^b = (\Delta^a \cap \Gamma) \cup \{j\}$ となり，$\Gamma \cap \Delta^{ab} \supseteqq (\Gamma \cap \Delta^a) \cup \{j\}$，したがって $|\Gamma \cap \Delta^{ab}| \gneqq |\Gamma \cap \Delta^a|$ となり $|\Gamma \cap \Delta^a|$ が最大であることに反する．

以上より $\Gamma \cap \Delta^a = \Gamma$ である．□

GをΩ上の可移群とする．$i \in \Omega$ に対してΩ上の G_i- 軌道を i におけるGの**部分軌道** (suborbit) という．

いま i における G の部分軌道を $\Delta_1(i)=\{i\}, \Delta_2(i), \cdots, \Delta_r(i)$ とする．任意の $j\in\Omega$ に対して，G は可移であるから $i^a=j$ となる $a\in G$ が存在する．このとき j における G の部分軌道は $\Delta_1(i)^a=\{i\}^a=\{j\}, \Delta_2(i)^a, \cdots, \Delta_r(i)^a$ である．このことより Ω の文字に関係なく G の部分軌道の個数は一定数 r である．この r を G の**部分軌道の個数** (rank) という．

定理 4.7 G を Ω 上の可移群，$i\in\Omega$ とする．このとき (G_i, G_i) による G の両側剰余類の個数と，G の部分軌道の個数は等しい．ここで

$$G=G_ix_1G_i+G_ix_2G_i+\cdots+G_ix_rG_i$$

とするとき，G_i- 軌道は $i^{x_1G_i}, i^{x_2G_i}, \cdots, i^{x_rG_i}$ である．

［証 明］ G は Ω 上可移だから，$\Omega=i^G=\bigcup_{k=1}^{r} i^{G_ix_kG_i}=\bigcup_{k=1}^{r} i^{x_kG_i}$ で，$i^{x_kG_i}$ $(k=1, 2, \cdots, r)$ は G_i- 軌道である．いま $i^{x_kG_i}=i^{x_{k'}G_i}$ とすると，$i^{x_k}=i^{x_{k'}a}$ となる $a\in G_i$ が存在する．したがって $x_k(x_{k'}a)^{-1}\in G_i$, $x_k\in G_ix_{k'}a\subseteqq G_ix_{k'}G_i$ となり $k=k'$ である．すなわち $i^{x_1G_i}, i^{x_2G_i}, \cdots, i^{x_rG_i}$ はすべて異なり，$\Omega=\bigcup_{k=1}^{r} i^{x_kG_i}$ は互いに素な G_i- 軌道による Ω の分割である．□

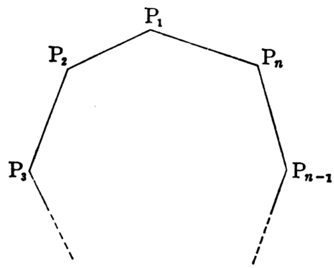
定理 4.7 よりつぎの系が成り立つ．

系 4.8 G を Ω 上の可移群とする．G が Ω 上2重可移であるための必要十分条件は

$$G=G_i+G_iaG_i$$

となることである．

2 面体群



2-5 図

正 n 角形において 2-5 図のように頂点を順次 $P_1, P_2, \cdots, P_n$ とする．また x を $\Omega=\{1, 2, \cdots, n\}$ 上の置換とする．いま置換 x により，頂点 P_i $(i=1, 2, \cdots, n)$ は頂点 P_{i^x} にうつるとする．このとき $P_{1^x}, P_{2^x}, \cdots, P_{n^x}$ をこの順に結ぶ図形 $P_{1^x}P_{2^x}\cdots P_{n^x}$ が，もとの正 n 角形 $P_1P_2\cdots P_n$ に一致するような置換 x 全体の集合を，D_{2n} とおく．明らかに $P_{1^x}, P_{2^x}, \cdots, P_{n^x}$ が，正 n 角形の頂点を P_{1^x} よりはじめて，左まわりまたは右まわりに順次並べたものであるとき，そのときに限り x は D_{2n} の元である．したがって $x, y\in D_{2n}$ に対して，$xy\in D_{2n}$

となり D_{2n} はΩ上の置換群になる．これを2面体群（dihedral group）という．

図形 $P_2P_3\cdots P_nP_1$ は

$$a=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ 2 & 3 & \cdots & n & 1\end{pmatrix}=(1\ 2\ \cdots\ n)$$

により図形 $P_1P_2\cdots P_n$ をうつしたもので，したがって $a\in D_{2n}$ である．このときaは正n角形を中心のまわりに，$2\pi/n$ 回転する置換であり，$\langle a\rangle$ は位数nでΩ上可移である．したがって D_{2n} もΩ上可移である．

D_{2n} における点1の安定化群をHとする．$x\in H$ は P_1 を固定するから，$P_{2^x}=P_2$ または $P_{2^x}=P_n$ である．$P_{2^x}=P_2$ のとき，xはすべての頂点を固定し $x=1$ である．$P_{2^x}=P_n$ となるxをbとおく．このとき $P_{n^b}=P_2$，$P_{3^b}=P_{n-1}$，$P_{n-1^b}=P_3$，… となり

$$b=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ 1 & n & n-1 & \cdots & 2\end{pmatrix}=(1)(2\ \ n)(3\ \ n-1)\cdots$$

となる．したがってnが偶数のとき，線分 $P_1P_{\frac{n+2}{2}}$ を軸にしたπ回転で

$$b=(1)(2\ \ n)\cdots\left(\frac{n}{2}\ \ \frac{n+4}{2}\right)\left(\frac{n+2}{2}\right)$$

である．nが奇数のとき，頂点 P_1 と辺 $P_{\frac{n+1}{2}}P_{\frac{n+3}{2}}$ の中点を結ぶ線分を軸にしたπ回転で

$$b=(1)(2\ \ n)\cdots\left(\frac{n+1}{2}\ \ \frac{n+3}{2}\right)$$

である．以上よりHは位数2の巡回群 $\langle b\rangle$ で

$$D_{2n}=H+Ha+\cdots+Ha^{n-1}=\{1, a, \cdots, a^{n-1}, b, ba, \cdots, ba^{n-1}\}$$

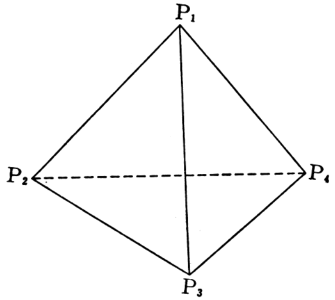
となり，D_{2n} の位数は $2n$ である．また $|D_{2n}:\langle a\rangle|=2$ であるから，$\langle a\rangle$ は D_{2n} における指数2の正規部分群である．

一般に2元 a, b で生成され，aの位数が n，b の位数が2で，$a^b=a^{-1}$ をみたす群を2面体群 D_{2n} という．

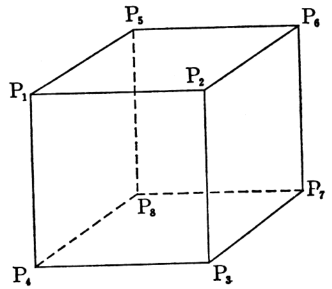
問 4.1 正n面体 $P_1P_2\cdots P_n$ に対して，x は $\{1, 2, \cdots, n\}$ 上の置換で，正n面体の頂点 P_i を P_{i^x} にうつすとする．いまこのような置換のうち，正n面体の回転をひきおこすもの全体の作る群を，正n面体群という．

（1） 正4面体群は，$\{1,2,3,4\}$ 上交代群 A_4 である．

（2） 正6面体群は，位数24で，$\{1,2,\cdots,8\}$ 上階数4の可移群である．さらに 2-7図



2-6 図



2-7 図

で向かい合った頂点を結ぶ4つの直線 $l_1 = P_1P_7$, $l_2 = P_2P_8$, $l_3 = P_3P_5$, $l_4 = P_4P_6$ をとり，正6面体群の元 x に対して，$l_1{}^x = P_{1^x}P_{7^x}$, …, $l_4{}^x = P_{4^x}P_{6^x}$ と定義すると，x は $\{l_1, l_2, l_3, l_4\}$ 上の置換をひきおこす．したがって $\{1, 2, 3, 4\}$ 上の置換 $\bar{x}$ を $l_i{}^x = l_{i^{\bar{x}}}$ $(i = 1, 2, 3, 4)$ により定義すると，$\bar{x}$ の全体は対称群 S_4 であることを示せ．

問 4.2 Gを $\Omega = \{1, 2, \cdots, n\}$ 上の置換群とする．GがΩ上 t 重可移 $(t \geqq 2)$ であるための必要十分条件は，GがΩ上可移で，G_1 が $\Omega - \{1\}$ 上 $t-1$ 重可移であることを示せ．

問 4.3 GをΩ上の可移群とする．GがΩ上2重可移であるための必要十分条件は，Gに位数2の部分群Hと，適当な文字 i が存在して，

$$G = G_iHG_i$$

となることを示せ．

§ 5. Witt の定理，Frobenius の定理

Gを一般の群，Ωを集合とする．群GからΩ上の対称群 S^Ω への準同型が存在するとき，GはΩに**作用**する．あるいはGをΩ上の作用といい，このことを (G, Ω) とも書く．

いまこの準同型をφとする．$x \in G$ に対して x^φ は Ω 上の置換であり，$i^{x^\varphi} (i \in \Omega)$ を単に i^x と書くことが多い．準同型φの核を作用の核といい，これをNとすると G/N は S^Ω の部分群と同型で，Ω上の置換群とみなすことができる．これより G/N のΩ上の軌道をGの軌道という．またΩの部分集合Δに対して $((G/N)_\Delta)^{\varphi^{-1}} = \{x \in G \mid i^x = i, \ {}^\forall i \in \Delta\}$ をGにおけるΔの安定化群と

いい，やはり G_Δ と書く．同様に $((G/N)_{(\Delta)})^{\varphi^{-1}}$ をGにおける集合としてのΔの安定化群といい $G_{(\Delta)}$ と書く．

つぎのことは容易にたしかめられる．

注 5.1 群GがΩに作用しているとする．このとき置換群と同じようにt重可移が定義される．また §2, §4 の置換群としての軌道，安定化群についての性質はすべてGにおいて成り立つ．ただ本書ではGがΩに作用すると断わらない限りGを置換群として扱うが，注意深く読めばほとんどの性質は作用していると考えても成り立つことがわかるであろう．

また作用の例として

注 5.2 GをΩ上の可移群，NをGの正規部分群とし，Ω上の N-軌道を $\Delta_1, \Delta_2, \cdots, \Delta_m$ とする．このとき $\Delta_i = \Delta_1^{a_i}$, $a_i \in G$ $(i = 1, 2, \cdots, m)$ で，Gは $\bar{\Omega} = \{\Delta_1, \Delta_2, \cdots, \Delta_m\}$ に作用する．

［証 明］ $1 \in \Delta_1$ としてよい．仮定より $\Omega = \Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_m$（互いに素）である．$G$は$\Omega$上可移であるから，$1^{a_i} \in \Delta_i$ なる $a_i \in G$ $(i = 1, 2, \cdots, m)$ が存在する．$N \trianglelefteq G$ より $a_iN = Na_i$，したがって $\Delta_i = (1^{a_i})^N = (1^N)^{a_i} = \Delta_1^{a_i}$ である．

任意の$x \in G$をとる．任意の Δ_i に対して $\Delta_i^x = (1^{a_iN})^x = (1^{a_ix})^N$ より，Δ_i^x も N-軌道である．さらに $\Delta_i \neq \Delta_j$のとき，$\Delta_i^x \neq \Delta_j^x$ である．したがってGから $\bar{\Omega} = \{\Delta_1, \Delta_2, \cdots, \Delta_m\}$ 上の対称群への写像φを $x^\varphi = \bar{x} = \begin{pmatrix} \Delta_1 & \Delta_2 & \cdots & \Delta_m \\ \Delta_1^x & \Delta_2^x & \cdots & \Delta_m^x \end{pmatrix}$ により定義できる．ここでxはΩの部分集合 Δ_i を部分集合 Δ_i^x にうつし，$\bar{x}$ は $\bar{\Omega}$ の元 Δ_i を $\bar{\Omega}$ の元 Δ_i^x にうつす．このとき

$$\begin{aligned}\overline{xy} &= \begin{pmatrix} \Delta_1 & \Delta_2 & \cdots & \Delta_m \\ \Delta_1^{xy} & \Delta_2^{xy} & \cdots & \Delta_m^{xy} \end{pmatrix} = \begin{pmatrix} \Delta_1 & \Delta_2 & \cdots & \Delta_m \\ \Delta_1^{x} & \Delta_2^{x} & \cdots & \Delta_m^{x} \end{pmatrix} \begin{pmatrix} \Delta_1^x & \Delta_2^x & \cdots & \Delta_m^x \\ \Delta_1^{xy} & \Delta_2^{xy} & \cdots & \Delta_m^{xy} \end{pmatrix} \\ &= \bar{x}\bar{y}\end{aligned}$$

であるから，φは準同型であり，Gは $\bar{\Omega}$ に作用する．□

ΔをΩの部分集合とするとき，$G_{(\Delta)}$ は Δ に作用する．この作用の核は G_Δ であるから $G_{(\Delta)}/G_\Delta$ はΔ上で考えたときΔ上の置換群となり，これを G^Δ と書く．G^Δ は $G_{(\Delta)}$ をΔに制限して考えたときにえられるΔ上の置換群のことである．またXを $G_{(\Delta)}$ の部分集合，xを $G_{(\Delta)}$ の元とするとき，同じようにXおよびxのΔ上への制限をそれぞれ X^Δ, x^Δ と書く．

例． $\Omega = \{1, 2, 3, 4, 5\}$ 上 $x = (1\ 2)(3\ 4\ 5)$，$y = (1\ 2)(3\ 4)(5)$ で，$\Delta = \{1, 2\}$ と

するとき，$x^{\Delta}=y^{\Delta}=(1\ 2)$ である．

GをΩ上の置換群とする．XをGの部分集合とし，Xのすべての元が固定するΩの文字の集合を，Xの**固定点集合**といい $F(X)$と書く．特に $X=\{x\}$ のとき $F(\{x\})$ を $F(x)$ と書く．

注 5.3 GをΩ上の置換群，X $(\neq \phi)$ をGの部分集合，uを G の元，Δ をΩの部分集合とする．このとき

（1） $F(G_{\Delta})\geqq\Delta$.

（2） $F(X)^u=F(X^u)$.

（3） $G_{(F(X))}\geqq N_G(X)$ で, $F(X)$ はいくつかの $N_G(X)$-軌道の和集合である．

［証 明］（1） 明らかであるが，一般に $F(G_{\Delta})=\Delta$ とはならない．

（2）
$$i\in F(X^u)\Longleftrightarrow i^{x^u}=i^{u^{-1}xu}=i,\ \forall x\in X\Longleftrightarrow i^{u^{-1}x}=i^{u^{-1}},\ \forall x\in X$$
$$\Longleftrightarrow i^{u^{-1}}\in F(X)\Longleftrightarrow i\in F(X)^u$$

より $F(X)^u=F(X^u)$ である．

（3） 任意の $y\in N_G(X)$ に対して $X^y=X$ であるから，（2）より $F(X)^y=F(X^y)=F(X)$，すなわち $y\in G_{(F(X))}$ である．これより $N_G(X)$ は $F(X)$ を集合として固定するから，$F(X)$ はいくつかの $N_G(X)$-軌道の和集合である．□

$\Omega^{(t)}=\{(i_1,\ i_2,\cdots,i_t)\,|\,i_k\in\Omega$ で，$(i_1,i_2,\cdots,i_t)$ は異なる t 個の文字からなる順列$\}$ とする．GをΩ上の置換群とするとき，$x\in G$ に対して $(i_1,\ i_2,\cdots,i_t)^x=(i_1{}^x,i_2{}^x,\cdots,i_t{}^x)$ と定義すると，明らかにGは $\Omega^{(t)}$ 上の置換群になる．これを $(G,\Omega^{(t)})$ と書く．GがΩ上 t 重可移であることと，G が $\Omega^{(t)}$ 上可移であることとは同値である．

注 5.4 GはΩ上の可移群で，その部分軌道の個数をrとするとき，$(G,\Omega^{(2)})$ の軌道の個数は $r-1$ である．

［証 明］ $(G,\Omega^{(2)})$ の軌道を $\Delta_1,\Delta_2,\cdots,\Delta_{r'-1}$ とする．$i\in\Omega$ を固定し，$\Delta_k(i)=\{j\in\Omega\,|\,(i,j)\in\Delta_k\}$ $(k=1,2,\cdots,r'-1)$ とおく．$(i,j),(i,j')\in\Omega^{(2)}$ に対して，$(i,j),(i,j')$ が同じ $(G,\Omega^{(2)})$-軌道に含まれるとき，そのときに限り j,j' は同じ $(G_i,\ \Omega-\{i\})$-軌道に含まれる．

したがって $\Delta_1(i),\Delta_2(i),\cdots,\Delta_{r'-1}(i)$ はすべて異なる $(G_i,\Omega-\{i\})$-軌道である．さ

らに任意の $(G_i, \Omega-\{i\})$-軌道 $\varDelta(i)$ に対して $\{(i,j)\in\Omega^{(2)}\,|\,j\in\varDelta(i)\}$ はある $(G,\Omega^{(2)})$-軌道に含まれる．以上より $(G_i, \Omega-\{i\})$-軌道の個数は $r'-1$, すなわち (G,Ω) の部分軌道の個数は r' となり，$r'=r$ である．□

注 5.4 において $\Omega\times\Omega=\Omega^{(2)}\cup\{(i,i)\,|\,i\in\Omega\}$ をとると G は $\Omega\times\Omega$ 上の置換群である．このとき $\{(i,i)\,|\,i\in\Omega\}$ は $(G,\Omega\times\Omega)$ の 1 つの軌道になるから，$(G,\Omega\times\Omega)$ の軌道の個数と (G,Ω) の部分軌道の個数は等しくなる．

つぎは Manning の定理の一般化で，証明の方法は Alperin による．

定理 5.5 G を Ω 上の t 重可移群，$X(\neq\phi)$ を $|F(X)|\geqq t$ である G の部分集合，$F(X)^{(t)}$ 上の $N_G(X)$-軌道を $\varDelta_1, \varDelta_2, \cdots, \varDelta_r$, $H=G_{1\,2\cdots t}$ とする．このとき H に含まれる X と G-共役な部分集合の集合 $C=\{X^x\,|\,x\in G, X^x\subseteqq H\}$ は，r 個の H-共役類 $C=C_1\cup C_2\cup\cdots\cup C_r$（互いに素）とわかれる．ここで各 $N_G(X)$-軌道 $\varDelta_k$ の 1 点 $(i_1{}^{(k)}, i_2{}^{(k)}, \cdots, i_t{}^{(k)})$ に対し，$(i_1{}^{(k)}, i_2{}^{(k)}, \cdots, i_t{}^{(k)})^{a_k}=(1,2,\cdots,t)$ となる $a_k\in G$ が存在して，$C_k=\{X^{a_kx}\,|\,x\in H\}$ である．

さらに $|\varDelta_k|=|N_G(H)|\cdot|C_k|/|H|$ である．

［証明］ 任意の $(i_1, i_2, \cdots, i_t)\in F(X)^{(t)}$ に対して，G は Ω 上 t 重可移だから，$(i_1, i_2, \cdots, i_k)^a=(1,2,\cdots,t)$ なる $a\in G$ が存在する．このとき注 5.3（2）を用いて $F(X^a)=F(X)^a\supseteqq\{i_1, i_2, \cdots, i_t\}^a=\{1,2,\cdots,t\}$ となり，$X^a\subseteqq H, X^a\in C$ である．

$F(X)^{(t)}$ 上の同じ $N_G(X)$-軌道に含まれる任意の 2 点 $(i_1, i_2, \cdots, i_t)$，$(j_1, j_2, \cdots, j_t)$ に対して，$(i_1, i_2, \cdots, i_t)^a=(j_1, j_2, \cdots, j_t)^b=(1,2,\cdots,t)$ である任意の $a, b\in G$ をとる．$(i_1, i_2, \cdots, i_t)$, $(j_1, j_2, \cdots, j_t)$ は同じ $N_G(X)$-軌道に属するから，$(i_1, i_2, \cdots, i_t)^x=(j_1, j_2, \cdots, j_t)$ である $x\in N_G(X)$ が存在する．このとき

$$(1,2,\cdots,t)^{a^{-1}xb}=(i_1, i_2, \cdots, i_t)^{xb}=(j_1, j_2, \cdots, j_t)^b=(1,2,\cdots,t)$$

となり，$a^{-1}xb\in H$, $xbH=aH$ である．したがって $x\in N_G(X)$ より $X^{xbH}=X^{bH}=X^{aH}$ である．

以上より $F(X)^{(t)}$ 上の $N_G(X)$-軌道 $\varDelta_k$ に対して，$(i_1{}^{(k)}, i_2{}^{(k)}, \cdots, i_t{}^{(k)})\in\varDelta_k$ をとり $(i_1{}^{(k)}, i_2{}^{(k)}, \cdots, i_t{}^{(k)})^{a_k}=(1,2,\cdots,t)$ である $a_k\in G$ により C における H-共役類 $C_k=X^{a_kH}$ が一意的に決まる．

任意の $X^x\in C$ をとる．$X^x\subseteqq H$ より $F(X)^x=F(X^x)\supseteqq F(H)\supseteqq\{1,2,\cdots,t\}$ である．したがって $(i_1, i_2, \cdots, i_t)^x=(1,2,\cdots,t)$ となる $(i_1, i_2, \cdots, i_t)\in F(X)^{(t)}$ が存在する．いま $(i_1, i_2, \cdots, i_t)$ を含む $N_G(X)$-軌道を $\varDelta_k$ とすると $X^x\in C_k$ である．すなわち

$C=C_1\cup C_2\cup\cdots\cup C_r$ となる.

$C_k=C_l$ とする. すなわち $X^{a_kH}=X^{a_lH}$ とする. すると $X^{a_k}=X^{a_lx}$ なる $x\in H$ が存在する. したがって $a_kx^{-1}a_l^{-1}\in N_G(X)$ となり,

$(i_1^{(k)},i_2^{(k)},\cdots,i_t^{(k)})^{a_k x^{-1} a_l^{-1}}=(1,2,\cdots,t)^{x^{-1}a_l^{-1}}=(1,2,\cdots,t)^{a_l^{-1}}=(i_1^{(l)},i_2^{(l)},\cdots,i_t^{(l)})$

より $\varDelta_k=\varDelta_l$ である. したがって $C=C_1\cup C_2\cup\cdots\cup C_r$ (互いに素) である.

補題 4.2 (2) より $(N_G(X)_{i_1^{(k)}\, i_2^{(k)}\,\cdots\, i_t^{(k)}})^{a_k}=N_G(X^{a_k})_{1\,2\cdots t}=N_H(X^{a_k})$ であり, 定理 1;2.1 (2) より $|C_k|=|H|/|N_H(X^{a_k})|$ であるから

$$|\varDelta_k|=\frac{|N_G(X)|}{|N_G(X)_{i_1^{(k)}\, i_2^{(k)}\,\cdots\, i_t^{(k)}}|}=\frac{|N_G(X)|}{|N_H(X^{a_k})|}$$

$$=\frac{|N_G(X)|}{|H|}\cdot\frac{|H|}{|N_H(X^{a_k})|}=\frac{|N_G(X)|\cdot|C_k|}{|H|}$$

である. □

系 5.6 (Witt) GをΩ上のt重可移群, $H=G_{12\cdots t}$, $X(\neq\phi)$ をHの部分集合とする. XとG-共役なHの部分集合がつねに X とH-共役であれば, $N_G(X)^{F(X)}$ は $F(X)$ 上t重可移である.

[**証 明**] 定理 5.5 においてC自身が1つの H-共役類になる. したがって定理 5.5 より $N_G(X)^{F(X)}$ は $F(X)^{(t)}$ 上可移, すなわち $F(X)$ 上 t 重可移である. □

定理 5.5, 系 5.6 でGにおける文字 1, 2, …, t の安定化群Hについて述べたが, Gはt重可移だから補題 4.2 (2) よりGにおける任意の異なる t 個の点の安定化群はHと共役である. したがって 1, 2, …, t はΩの任意の異なる t 個の文字として扱えばよい.

Witt の定理は可移群における重要な定理である. この定理は定理 5.5 を用いなくても同じような証明ではあるが簡単に証明される.

[**系 5.6 の別証明**] Gはt重可移だから任意の $(i_1,i_2,\cdots,i_t)\in F(X)^{(t)}$ に対して, $(i_1,i_2,\cdots,i_t)^x=(1,2,\cdots,t)$ となる $x\in G$ が存在する. このとき

$$F(X^x)=F(X)^x\supseteqq\{i_1,i_2,\cdots,i_t\}^x=\{1,2,\cdots,t\}$$

である. したがって $X^x\subseteqq H$ となり仮定より $X^x=X^a$ となる $a\in H$ が存在する. これより $X^{xa^{-1}}=X$, $xa^{-1}\in N_G(X)$ となり, $(i_1,i_2,\cdots,i_t)^{xa^{-1}}=(1,2,\cdots,t)^{a^{-1}}=(1,2,\cdots,t)$, すなわち $N_G(X)^{F(X)}$ は $F(X)$ 上 t 重可移である. □

Witt の定理におけるXとして H, H の p-シロー部分群 (定義は §6) が

あるが，一般化した形で§8で述べる．

系 5.7　GをΩ上の可移群，$H=G_1, X(\neq\phi)$ をGの部分集合，$C=\{X^x|x\in G, X^x\subseteqq H\}$ とする．このとき

$$|F(X)|=|N_G(X)|\cdot|C|/|H|$$

である．

［証明］ $|F(X)|=0$ であれば，$|C|=0$ であるから定理は成り立つ．

$|F(X)|\neq 0$ とする．定理 5.5 において $t=1$ とし，$F(X)$ 上の $N_G(X)$- 軌道を $\Delta_1, \Delta_2, \cdots, \Delta_r$，$C$における$H$-共役類を $C_1, C_2, \cdots, C_r$ とする．このとき定理 5.5 より

$$|\Delta_k|=\frac{|N_G(X)|\cdot|C_k|}{|H|}, \qquad (k=1,2,\cdots,r)$$

である．したがって

$$|F(X)|=\sum_{k=1}^{r}|\Delta_k|=\frac{|N_G(X)|}{|H|}\sum_{k=1}^{r}|C_k| = \frac{|N_G(X)|\cdot|C|}{|H|}$$

である．□

定理 5.8 (Frobenius)　GをΩ上の置換群とする．$x\in G$ を巡回表示したときの長さ i の巡回成分の個数を $\alpha_i(x)$ と書く．このとき

$$\sum_{x\in G}\binom{\alpha_1(x)}{n_1}\binom{\alpha_2(x)}{n_2}\cdots\binom{\alpha_r(x)}{n_r}=\frac{m\cdot|G|}{1^{n_1}\cdot n_1!\cdot 2^{n_2}\cdot n_2!\cdots r^{n_r}\cdot n_r!}$$

である．

ここで$\binom{\alpha_i(x)}{n_i}$は $\alpha_i(x)$ 個から n_i 個をえらぶ組合せの個数で，$\alpha_i(x)\lneqq n_i$ のときは0とする．

またmはつぎのようにしてえられた正の整数である．$t=n_1+2n_2+\cdots+rn_r$ とし，Gの元を巡回表示したときに，

$$(i_1)\cdots(i_{n_1})(j_1\ j_1')\cdots(j_{n_2}\ j_{n_2}')\cdots(k_1^{(1)}\cdots k_1^{(r)})\cdots(k_{n_r}^{(1)}\cdots k_{n_r}^{(r)})\cdots$$

なる元がGに存在するとき，$\Omega^{(t)}$ の文字 $(i_1, \cdots, i_{n_1}, j_1, j_1', \cdots, j_{n_2}, j_{n_2}', \cdots, k_1^{(1)}, \cdots, k_1^{(r)}, \cdots, k_{n_r}^{(1)}, \cdots, k_{n_r}^{(r)})$ の集合をΓとおく．このときGはΓに作用し，Γにおける G-軌道の個数がmである．

［証明］ 任意の $\gamma\in\Gamma$ をとる．このときγがΓの文字であることを定める $a\in G$ が存在し，任意の $x\in G$ に対して補題3.1より a^x とΓの文字γ^x が対応する．したがってxはΓ上の置換となり，明らかに GはΓ に作用する．

いまGとΓの直積集合 $G\times\Gamma$の部分集合

$$S=\{(x,\gamma)\,|\,x=(i_1)\cdots(i_{n_1})(j_1\,j_1')\cdots(j_{n_2}\,j_{n_2}')\cdots(k_1^{(1)}\cdots k_1^{(r)})\cdots(k_{n_r}^{(1)}\cdots k_{n_r}^{(r)})\cdots \in G,\ \gamma=(i_1,\cdots,i_{n_1},j_1,j_1',\cdots,j_{n_2},j_{n_2}',\cdots,k_1^{(1)},\cdots,k_1^{(r)},\cdots,k_{n_r}^{(1)},\cdots,k_{n_r}^{(r)})\in\Gamma\}$$

を考え，S の元の個数を 2 通りの方法で数える．

G の元 x を固定し，x に対応する Γ の元の集合 $S(x,*)=\{\gamma\in\Gamma\,|\,(x,\gamma)\in S\}$ をとるとき

$$|S(x,*)|=\binom{\alpha_1(x)}{n_1}\binom{\alpha_2(x)}{n_2}\cdots\binom{\alpha_r(x)}{n_r}\cdot 1^{n_1}\cdot n_1!\cdot 2^{n_2}\cdot n_2!\cdots r^{n_r}\cdot n_r!$$

であるが，このことはつぎのようにして求められる．

$\binom{\alpha_1(x)}{n_1}\binom{\alpha_2(x)}{n_2}\cdots\binom{\alpha_r(x)}{n_r}\cdot n_1!\cdots n_2!\cdots n_r!$ において $\binom{\alpha_i(x)}{n_i}\cdot n_i!$ $(i=1,2,\cdots,r)$ は x の $\alpha_i(x)$ 個の i-巡回置換から n_i 個をえらんで並べる順列の個数である．ここで $\alpha_i(x)\lneqq n_i$ のときこの式の値は 0 である．

つぎに巡回置換の並べ方を 1 つ決める．このとき並べられた各 i- 巡回置換において，その巡回置換を作る i 個の文字のどれから巡回置換を書き始めるかによって i 通りの書く方法がある．したがって，n_i 個の i- 巡回置換に対して i^{n_i} 個の書き方が存在し，全体で $1^{n_1}\cdot 2^{n_2}\cdots r^{n_r}$ 個の並べ方がある．

したがって，$S=\bigcup_{x\in G}\{(x,\gamma)\,|\,\gamma\in S(x,*)\}$（互いに素）であるから

$$|S|=\sum_{x\in G}|S(x,*)|$$

$$=1^{n_1}\cdot n_1!\cdot 2^{n_2}\cdot n_2!\cdots r^{n_r}\cdot n_r!\sum_{x\in G}\binom{\alpha_1(x)}{n_1}\binom{\alpha_2(x)}{n_2}\cdots\binom{\alpha_r(x)}{n_r} \qquad ①$$

である．

つぎに Γ の文字 $\gamma=(i_1,\cdots,i_{n_1},j_1,j_1',\cdots,j_{n_2},j_{n_2}',\cdots,k_1^{(1)},\cdots,k_1^{(r)},\cdots,k_{n_r}^{(1)},\cdots,k_{n_r}^{(r)})$ を固定し，γ に対応する G の元の集合 $S(*,\gamma)=\{x\in G\,|\,(x,\gamma)\in S\}$ をとり，列 γ を作る t 個の文字の安定化群を G_γ とおく．$S(*,\gamma)$ の元 a を定めると，G の元 x が $x\in G_\gamma\cdot a$ であるときそのときに限り $x\in S(*,\gamma)$ であるから，$|S(*,\gamma)|=|G_\gamma|$ である．ここで $S=\bigcup_{\gamma\in\Gamma}\{(x,\gamma)\,|\,x\in S(*,\gamma)\}$（互いに素）であるから

$$|S|=\sum_{\gamma\in\Gamma}|G_\gamma|$$

である．

いま Γ 上の G- 軌道を，$\Delta_1,\Delta_2,\cdots,\Delta_m$ とし，各 Δ_i より代表元 γ_i をとる．Γ の文字 γ と γ' が同じ G- 軌道に属するならば，$|G_\gamma|=|G_{\gamma'}|$ であるから上式より

$$|S|=\sum_{i=1}^{m}|\Delta_i|\cdot|G_{\gamma_i}|$$

である．さらに Δ_i は G- 軌道だから，系 4.4 より $|G|=|\Delta_i|\cdot|G_{\gamma_i}|$ である．よって

$$|S|=\sum_{i=1}^{m}|G|=m\cdot|G| \qquad ②$$

である．以上より$|S|$についての２つの式①，②より求める等式がえられる．□

集合の元の個数を数える際に，定理5.8の証明で用いた方法がよくとられる．すなわち A, B を集合，SをAとBの直積集合 $A\times B$ の部分集合とする．

$$S(a,*)=\{b\in B\,|\,(a,b)\in S\},\qquad S(*,b)=\{a\in A\,|\,(a,b)\in S\}$$

とおくとき

$$S=\bigcup_{a\in A}\{(a,b)\,|\,b\in S(a,*)\}(\text{互いに素})=\bigcup_{b\in B}\{(a,b)\,|\,a\in S(*,b)\}(\text{互いに素})$$

であるから，Sの元の個数をつぎの２通りに示すことができる．

$$|S|=\sum_{a\in A}|S(a,*)|=\sum_{b\in B}|S(*,b)|.$$

系 5.9 （１） Gがt重可移群で，$r\leqq t$ のとき

$$\sum_{x\in G}\alpha_r(x)=\frac{1}{r}|G|$$

である．

（２） Gがm個の軌道をもつとき

$$\sum_{x\in G}|F(x)|=m\cdot|G|$$

である．

（３） Gが可移群で，Gの部分軌道の個数をmとするとき

$$\sum_{x\in G}|F(x)|^2=m\cdot|G|$$

である．

［証明］（１） GはΩ上t重可移で，$r\leqq t$ であるから，$\Gamma=\{(i_1, i_2,\cdots,i_r)\,|\,(i_1\,i_2\cdots i_r)\cdots\in G$ (巡回表示)$\}$ の上で可移である．したがって定理5.8より

$$\sum_{x\in G}\alpha_r(x)=\sum_{x\in G}\binom{\alpha_r(x)}{1}=\frac{|G|}{r\cdot 1!}=\frac{1}{r}\cdot|G|$$

である．

（２） $\Gamma=\{i\,|\,x=(i)\cdots\in G$ (巡回表示)$\}$ において，xとしてGの単位元をとることにより $\Gamma=\Omega$ である．$|F(x)|=\alpha_1(x)$ だから定理5.8より

$$\sum_{x\in G}|F(x)|=\sum_{x\in G}\binom{\alpha_1(x)}{1}=m\cdot|G|$$

である．

（３） 定理5.8より

$$\sum_{x\in G}\binom{\alpha_1(x)}{2}=\frac{1}{2}m'\cdot|G|$$

である．$\Gamma=\{(i_1,i_2)\,|\,(i_1)(i_2)\cdots\in G$ (巡回表示)$\}$は，（２）と同様に単位元をとること

により $\Omega^{(2)}$ に等しい.

GはΩ上可移であるから，任意の $(i, j) \in \Omega^{(2)}$ に対して$i^x = 1$ である $x \in G$ が存在し，$(i, j)^x = (1, j^x)$ である．さらに $(1, j)$ と (i, j') が同じ G- 軌道に属すということと，j, j' が同じ G_1- 軌道に属すということは同値であるから，$\Omega^{(2)}$ 上の G- 軌道の個数 m' は，$\Omega - \{1\}$ 上の G_1- 軌道の個数 $m-1$ に等しい．したがって

$$\frac{1}{2}\cdot m'\cdot|G| = \frac{1}{2}(m-1)|G| \qquad ①$$

である．また

$$\sum_{x\in G}\binom{\alpha_1(x)}{2} = \frac{1}{2}\sum_{x\in G}\alpha_1(x)(\alpha_1(x)-1) = \frac{1}{2}(\sum_{x\in G}\alpha_1(x)^2 - \sum_{x\in G}\alpha_1(x))$$

である．ここでGはΩ上可移であるから（2）より $\sum_{x\in G}\alpha_1(x) = |G|$ である．すなわち上式の右辺は

$$\frac{1}{2}(\sum_{x\in G}\alpha_1(x)^2 - |G|) \qquad ②$$

に等しい．したがって①，②より

$$\frac{1}{2}(m-1)|G| = \frac{1}{2}(\sum_{x\in G}\alpha_1(x)^2 - |G|)$$

が成り立ち，$\alpha_1(x) = |F(x)|$ より

$$\sum_{x\in G}|F(x)|^2 = m\cdot|G|$$

をうる．□

問 5.1 Gを $\{1, 2, \cdots, 8\}$ 上の4元数群 $\langle a, b\rangle$, $a = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$, $b = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$ とする．$\Gamma = \{(i, j) \in \Omega^{(2)} \mid \exists(i\ j)\cdots \in G\}$ とおくとき，GはΓ上可移に作用することを示せ．

問 5.2 Gを§4 であげた $\Omega = \{1, 2, \cdots, 2n\}$ 上の2面体群 D_{2n} とする．このときGを $\Omega^{(3)}$ 上の置換群とみなしたときの軌道の個数を求めよ．

問 5.3 Gを3重可移群とするとき，$\sum_{x\in G}|F(x)|^3 = 5\cdot|G|$ となることを示せ．

問 5.4 GをΩ上の置換群，HをGの部分群，UをHの部分群とする．いま $F(H) \neq \phi$ とし，Uと G- 共役なHの部分群はつねにUと H- 共役であれば，$N_G(U)$ の部分群Nで，$N \leqq G_{(F(H))}$, $N^{F(H)} = N_G(H)^{F(H)}$ となるものが存在することを示せ．

§6. 群の置換表現

置換群 (G, Ω) と (G', Ω') において，Gから G' への全単射f，およびΩから Ω' への全単射φが存在するとする．いま任意の $x \in G$ と任意の $i \in \Omega$ に対して

$$(i^x)^\varphi = (i^\varphi)^{x^f}$$

が成り立つとき，置換群 (G, Ω) と (G', Ω') は**同値な置換群**であるといい

$$(G, \Omega) \cong (G', \Omega')$$

と書く．

このとき任意の $x, y \in G$，任意の $i' \in \Omega'$ に対して，$i'^{\varphi^{-1}} = i$ とすると

$$i'^{(xy)^f} = (i^\varphi)^{(xy)^f} = (i^{xy})^\varphi = ((i^x)^y)^\varphi = ((i^x)^\varphi)^{y^f} = ((i^\varphi)^{x^f})^{y^f} = i'^{x^f y^f}$$

であるから $(xy)^f = x^f y^f$ が成り立つ．したがって

注 6.1 (G, Ω) と (G', Ω') が同値な置換群であれば，GとG'は群として同型である．

一般の群Gから対称群 S^Ω の中への準同型を，G の Ω 上の**置換表現**という．

φをGの Ω 上の置換表現とする．G^φ がΩ上可移のとき，φを**可移表現**という．またφが同型のとき，置換表現φは**忠実**であるという．

補題 6.2 Gを一般の群，HをGの部分群，GのHによる左分解を

$$G = Ha_1 + Ha_2 + \cdots + Ha_n$$

とする．$\Omega = G/H = \{Ha_1, Ha_2, \cdots, Ha_n\}$ とおくと，$x \in G$ に対してΩ上の置換

$$x^* = \begin{pmatrix} Ha_1 & Ha_2 & \cdots & Ha_n \\ Ha_1x & Ha_2x & \cdots & Ha_nx \end{pmatrix}$$

が定義できる．このとき $G^* = \{x^* | x \in G\}$ はΩ上の置換群で，写像 $G \to G^*$，$x \mapsto x^*$ はGのΩ上の置換表現である．

［証 明］ xをGの元とする．任意の $Ha_i \in \Omega$ に対して Ha_ix はまたHの左剰余類であるから，$Ha_ix \in \Omega$ である．また $Ha_ix = Ha_{i'}x$ であれば $Ha_i = Ha_{i'}$ である．したがって x^* はΩ上の置換である．

写像 $G \to G^*, x \mapsto x^*$ はGから対称群 S^Ω の中への写像で，任意の $x, y \in G$ に対して

$$\begin{aligned}(xy)^* &= \begin{pmatrix} Ha_1 & Ha_2 & \cdots & Ha_n \\ Ha_1xy & Ha_2xy & \cdots & Ha_nxy \end{pmatrix} \\ &= \begin{pmatrix} Ha_1 & Ha_2 & \cdots & Ha_n \\ Ha_1x & Ha_2x & \cdots & Ha_nx \end{pmatrix} \begin{pmatrix} Ha_1x & Ha_2x & \cdots & Ha_nx \\ Ha_1xy & Ha_2xy & \cdots & Ha_nxy \end{pmatrix} \\ &= x^*y^*\end{aligned}$$

である．したがって写像 $G \to G^*$ は準同型になり，GのΩ上の置換表現である．□

補題 6.2 の置換表現を**部分群Hによる（右）置換表現**，またはGの**G/H上の置換表現**といい，(G^*, Ω) を $(G, G/H)$ とも書く．

例 1. Gを対称群 S_n，Gの部分群Hとして交代群 A_n をとる．このとき $S_n = A_n + A_n(1\ 2)$ であるから，S_n の $\Omega = \{A_n, A_n(1\ 2)\}$ 上の置換表現は，$x \in A_n$ のとき $x^* = \begin{pmatrix} A_n & A_n(1\ 2) \\ A_n x & A_n(1\ 2)x \end{pmatrix} = \begin{pmatrix} A_n & A_n(1\ 2) \\ A_n & A_n(1\ 2) \end{pmatrix}$，$x \notin A_n$ のとき $x^* = \begin{pmatrix} A_n & A_n(1\ 2) \\ A_n x & A_n(1\ 2)x \end{pmatrix} = \begin{pmatrix} A_n & A_n(1\ 2) \\ A_n(1\ 2) & A_n \end{pmatrix}$ となる．すなわち S_n は $\{A_n, A_n(1\ 2)\}$ 上の置換群 $\left\{1, \begin{pmatrix} A_n & A_n(1\ 2) \\ A_n(1\ 2) & A_n \end{pmatrix}\right\}$ として置換表現される．このように対称群 S_n を次数2の置換群として表現することができる．したがって置換群Gといったとき，その次数により置換の表し方は，当然異なってくる．この混乱をさけるため，本書では対称群 S_n，交代群 A_n というときは，特に断わらない限り次数nとする．

定理 6.3 群Gの部分群Hによる置換表現は，可移表現でその表現の核は $\bigcap_{x\in G} H^x$ である．

［**証明**］ $G/H = \{Ha_1, Ha_2, \cdots, Ha_n\}$, $G^* = \left\{x^* = \begin{pmatrix} Ha_i \\ Ha_i x \end{pmatrix} \middle| \ x \in G\right\}$ とする．任意の $Ha_i \in G/H$ に対して，$Ha_i = Ha_1(a_1^{-1}\ a_i) = Ha_1^{(a_1^{-1}\ a_i)^*}$ だから，定理 2.3 よりG^*は G/H 上可移である．

$a \in G$ に対して，

$$a^* = 1 \Longleftrightarrow Ha_i a = Ha_i, \forall Ha_i \in G/H \Longleftrightarrow Hxa = Hx, \forall x \in G$$
$$\Longleftrightarrow x^{-1}Hxa = x^{-1}Hx, \forall x \in G \Longleftrightarrow a \in \bigcap_{x\in G} H^x$$

である．したがって部分群Hによる置換表現の核は $\bigcap_{x\in G} H^x$ である．□

群の単位群1による置換表現を（右）**正則表現**という．群 G の正則表現による置換群は，$(G, G/1)$ である．

例 2. 位数4の群$G = \{a_1 = 1, a_2 = (1\ 2), a_3 = (3\ 4), a_4 = (1\ 2)(3\ 4)\}$の正則表現は

$$a_2^* = \begin{pmatrix} 1 & (1\ 2) & (3\ 4) & (1\ 2)(3\ 4) \\ (1\ 2) & 1 & (1\ 2)(3\ 4) & (3\ 4) \end{pmatrix} = (a_1\ a_2)(a_3\ a_4)$$

$$a_3^* = \begin{pmatrix} 1 & (1\ 2) & (3\ 4) & (1\ 2)(3\ 4) \\ (3\ 4) & (1\ 2)(3\ 4) & 1 & (1\ 2) \end{pmatrix} = (a_1\ a_3)(a_2\ a_4)$$

$$a_4^* = \begin{pmatrix} 1 & (1\ 2) & (3\ 4) & (1\ 2)(3\ 4) \\ (1\ 2)(3\ 4) & (3\ 4) & (1\ 2) & 1 \end{pmatrix} = (a_1\ a_4)(a_2\ a_3)$$

となり，{1, 2, 3, 4} 上 $G^* = \{a_1{}^* = 1,\ a_2{}^* = (1\ 2)(3\ 4),\ a_3{}^* = (1\ 3)(2\ 4),\ a_4{}^* = (1\ 4)(2\ 3)\}$ である．

注 6.4 正則表現 $G \to G^*$ は忠実な表現で，G^* の元（$\neq 1$）は固定点をもたない（§11 で述べるが，可移群で単位元以外の元が固定点をもたないとき正則という）．したがってGの任意の部分群Hに対応する G^* の部分群 $H^* = \{x^* \in G^* \mid x \in H\}$ の軌道の長さは，すべて$|H|$に等しい．

［**証明**］ G^* は $\Omega = G/1 = \{a_1, a_2, \cdots, a_n\}$ 上の置換群である．したがって $\bigcap_{x \in G} 1^x = 1$ だから定理 6.3 より，正則表現は忠実である．$x \neq 1$ のとき任意の a_i に対して $a_i x \neq a_i$ であるから，x^* はΩ上に固定点をもたない．

Gの部分群Hに対して，ΔをΩ上の H^*-軌道とする．$a \in \Delta$ に対して，上で述べたことより a の安定化群 $H^*{}_a = 1$ だから，系 4.4 より $|\Delta| = |H^* : H^*{}_a| = |H^*| = |H|$ である．□

Hを群Gの部分群とし，Hの右剰余類の集合を $\Omega = \{b_1H, b_2H, \cdots, b_nH\}$ とおく．このとき $x \in G$ に対してΩ上の置換

$$^*x = \begin{pmatrix} b_1H & b_2H & \cdots & b_nH \\ x^{-1}b_1H & x^{-1}b_2H & \cdots & x^{-1}b_nH \end{pmatrix}$$

が定義できる．このとき任意の $x, y \in G$ に対して

$$\begin{aligned} ^*(xy) &= \begin{pmatrix} b_1H & b_2H & \cdots & b_nH \\ (xy)^{-1}b_1H & (xy)^{-1}b_2H & \cdots & (xy)^{-1}b_nH \end{pmatrix} \\ &= \begin{pmatrix} b_1H & b_2H & \cdots & b_nH \\ x^{-1}b_1H & x^{-1}b_2H & \cdots & x^{-1}b_nH \end{pmatrix} \\ &\quad \times \begin{pmatrix} x^{-1}b_1H & x^{-1}b_2H & \cdots & x^{-1}b_nH \\ y^{-1}x^{-1}b_1H & y^{-1}x^{-1}b_2H & \cdots & y^{-1}x^{-1}b_nH \end{pmatrix} = {}^*x{}^*y \end{aligned}$$

である．したがって $^*G = \{^*x \mid x \in G\}$ はΩ上の置換群で，写像 $G \to {}^*G,\ x \mapsto {}^*x$ は準同型になる．この写像をGの**部分群Hによる左置換表現**という．

定理 6.5 φを群Gの $\Omega = \{1, 2, \cdots, n\}$ 上の可移置換表現とし，

$$H = ((G^\varphi)_1)^{\varphi^{-1}} = \{x \in G \mid 1^{x^\varphi} = 1\}$$

とおく．このとき $(G^\varphi, \Omega) \cong (G, G/H)$ で，$\ker \varphi = \bigcap_{x \in G} H^x$ である．

［**証明**］ GのΩ上への作用において，文字1の安定化群がHである．G^φ はΩ上可移だから，定理 4.3 (1) および注 5.1 より $1^{x_i{}^\varphi} = i$ となる元 x_i がGに存在して，$G = Hx_1 + Hx_2 + \cdots + Hx_n$ と左分解される．ここで $Hx_i = \{x \in G \mid 1^{x^\varphi} = i\}$ である．

Gの部分群Hによる置換表現を $G\to G^*, x\mapsto x^*$ とする. $\Omega=\{1,2,\cdots,n\}$ と$\Omega^*=\{H=Hx_1, Hx_2,\cdots,Hx_n\}$ との間に $i\leftrightarrow Hx_i$ により1対1対応を与える. この対応において $1^{x^\varphi}=i$ のとき $Hx=Hx_i$ であるから $1^{x^\varphi}\leftrightarrow Hx$ である.

任意の2元 $x,y\in G$ に対して

$$x^\varphi=y^\varphi\Longleftrightarrow i^{x^\varphi}=i^{y^\varphi}, {}^\forall i\in\Omega\Longleftrightarrow 1^{x_i{}^\varphi x^\varphi}=1^{x_i{}^\varphi y^\varphi}, i=1,2,\cdots,n$$

$$\Longleftrightarrow 1^{(x_i x)^\varphi}=1^{(x_i y)^\varphi}, i=1,2,\cdots,n\Longleftrightarrow Hx_ix=Hx_iy, i=1,2,\cdots,n\Longleftrightarrow x^*=y^*$$

である. したがって写像 $G^\varphi\to G^*$ を $x^\varphi\mapsto x^*$ により定義できて, この写像は全単射である.

任意の $i\in\Omega$ に対して, i^{x^φ} に対応する Ω^* の文字は $i^{x^\varphi}=1^{(x_ix)^\varphi}$ より Hx_ix である. 一方 i に対応する Ω^* の文字 Hx_i に対して, x^φ に対応する x^* により $(Hx_i)^{x^*}=Hx_ix$ である. したがって $(G^\varphi,\Omega)\cong(G^*,\Omega^*)=(G,G/H)$ である.

Gの元xがφの核の元であるとき, そのときに限り $x^*=1$ であるから, φの核は部分群Hによる置換表現の核と一致し, 定理6.3より $\bigcap_{x\in G}H^x$ である. □

系 6.6 $X\ (\neq\phi)$ をGの部分集合とし, XとG-共役な部分集合全体の集合を $\Omega=\{X=X_1, X_2,\cdots,X_n\}$ とおく.

このとき $x\in G$ に対してΩ上の置換

$$\bar{x}=\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1{}^x & X_2{}^x & \cdots & X_n{}^x \end{pmatrix}$$

が定義できる. これより $\bar{G}=\{\bar{x}\mid x\in G\}$ はΩ上の可移置換群で, $(\bar{G},\Omega)\cong(G, G/N_G(X))$ である.

[証 明] ΩはXと共役な部分集合全体からなる集合だから, $\bar{x}$は明らかにΩ上の置換である. 任意の2元 $x,y\in G$ に対して

$$\overline{xy}=\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1{}^{xy} & X_2{}^{xy} & \cdots & X_n{}^{xy} \end{pmatrix}=\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1{}^x & X_2{}^x & \cdots & X_n{}^x \end{pmatrix}\begin{pmatrix} X_1{}^x & X_2{}^x & \cdots & X_n{}^x \\ X_1{}^{xy} & X_2{}^{xy} & \cdots & X_n{}^{xy} \end{pmatrix}$$
$$=\bar{x}\,\bar{y}$$

であるから, $\bar{G}$ はGのΩ上の置換表現によりえられる. Ωの文字はXと共役な部分集合だから, $\bar{G}$ はΩ上可移である.

$\{x\in G\mid X^x=X\}=N_G(X)$ であるから, 定理6.5より $(\bar{G},\Omega)\cong(G, G/N_G(X))$ である. □

つぎに置換群の性質を用いた Wielandt の方法によるシローの定理の証明について述べる.

群Gの位数が素数pに対して $p^r m,\ (p,m)=1$ のとき，位数が p^r であるGの部分群を **p-シロー部分群** (Sylow p-subgroup) という．

定理 6.7 (Sylow) (1) p^t がGの位数を約するとき，Gは位数 p^t の部分群をもち，この部分群はGのある p-シロー部分群に含まれる．

(2) Gの p-シロー部分群はすべて共役である．

(3) Gの p-シロー部分群の個数は $1+kp$ $(k\geqq 0)$ である．

(1) の前半および (3) を拡張したつぎの定理を証明する．

定理 6.8 p^t が群Gの位数を約するとき，Gの位数 p^t の部分群の個数は $1+kp$ $(k\geqq 0)$ である．

［証明］ $|G|=p^r m,\ (p,m)=1$ とすると $r\geqq t$ である．いまGの正則表現によりGを$G/1$上の置換群とみなし，XをGの p^t 個の元からなるGの部分集合とする．このときXは，Xの集合としての安定化群 $G_{(X)}$ のいくつかの軌道の和集合となり，注 6.4 より $G_{(X)}$ -軌道の長さはすべて $|G_{(X)}|$ に等しい．したがって $|X|=p^t$ であるから，$|G_{(X)}|=p^s$, $s\leqq t$ となり，特に $s=t$ になるのは $G_{(X)}$ が X 上可移のときである．

いま Ω をGの p^t 個の元からなる部分集合全体の集合とすると，G の元による Ω 上の置換が $\begin{pmatrix} X \\ Xa \end{pmatrix}$，$X\in\Omega$, $a\in G$ により定義できる．したがってGはΩに作用し，Ω 上のG-軌道を $\Delta_1,\Delta_2,\cdots,\Delta_n$ とし，さらに各 Δ_i より X_i をとる．このとき $|G_{(X_i)}|=p^{s_i}$, $s_i\leqq t$ であるから $|\Delta_i|=|G:G_{(X_i)}|=p^{r-s_i}m$ である．

Hを位数 p^t のGの部分群とすると，$H\in\Delta_i$ となるG-軌道 Δ_i が存在し，$G_{(H)}=H$ より $|\Delta_i|=p^{r-t}m$ ，$\Delta_i=G/H$ である．逆に $|\Delta_i|=p^{r-t}m$ とする．$a_i\in X_i$ に対して $1\in X_i a_i^{-1}\in\Delta_i$ となり $X_i a_i^{-1}$ をあらためて X_i とおく．このとき $|G_{(X_i)}|=|G|/|\Delta_i|=p^t$ で，$G_{(X_i)}$ は X_i 上可移になり，$1\in X_i$ より $X_i=1\cdot G_{(X_i)}=G_{(X_i)}$，したがって X_i はGの部分群になり，$\Delta_i=G/G_{(X_i)}$である．以上よりGにおける位数 p^t の部分群と，$|\Delta_i|=p^{r-t}m$ であるΩ上のG-軌道が1対1に対応し，いまその個数を l とする．

このとき

$$|\Omega|=\sum_{i=1}^{n}|\Delta_i|=\sum_{i=1}^{n}p^{r-s_i}m=\sum_{s_i=t}{}' p^{r-s_i}m+\sum_{s_i<t}{}'' p^{r-s_i}m$$
$$=p^{r-t}m\cdot l+p^{r-t}m\sum_{s_i<t}{}'' p^{t-s_i}=p^{r-t}m(l+k'p) \qquad ①$$

である．

一方Ωは p^t 個の元からなるGの部分集合すべてよりなるから

$$|\Omega|=\binom{p^r m}{p^t}=\prod_{j=0}^{p^t-1}\frac{p^r m-j}{p^t-j}=p^{r-t}m\prod_{j=1}^{p^t-1}\frac{p^r m-j}{p^t-j} \qquad ②$$

である．したがって①，②より $l+k'p=\prod_{j=1}^{p^t-1}\dfrac{p^r m-j}{p^t-j}$ となる．ここで $j=p^{r_j}\cdot m_j$，$(p, m_j)=1$ とすると，$r_j<t$ で

$$\frac{p^r m-j}{p^t-j}=\frac{p^{r-r_j}m-m_j}{p^{t-r_j}-m_j}=\frac{p^{r-r_j}m-p^{t-r_j}}{p^{t-r_j}-m_j}+1=\frac{p^{t-r_j}(p^{r-t}m-1)}{p^{t-r_j}-m_j}+1$$

である．したがって

$$l+k'p=\prod_{j=1}^{p^t-1}\left(\frac{p^{t-r_j}(p^{r-t}m-1)}{p^{t-r_j}-m_j}+1\right)=\frac{p\cdot k''}{\prod_{j=1}^{p^t-1}(p^{t-r_j}-m_j)}+1$$

となり $\left(\prod_{j=1}^{p^t-1}(p^{t-r_j}-m_j), p\right)=1$ であるから，右辺は $pk'''+1$ となる．すなわち $l=1+kp$ である．□

［**定理 6.7 の証明**］ 定理 6.7 の（1）の前半および（3）は定理 6.8 よりえられる．したがって（1）の後半と（2）を証明する．

PをGの p- シロー部分群，QをGの任意の p- 部分群とする．GのPによる置換表現を考える．$(G, G/P)$ において $(|G/P|, p)=1$ で，Qは p- 群であるから，Qは固定点をもつ．すなわち $PaQ=Pa$ である剰余類 Pa が存在する．このとき $a^{-1}PaQ=a^{-1}Pa$，$Q\leqq a^{-1}Pa$ となり $a^{-1}Pa$ もGの p- シロー群だから（1）の後半が成り立つ．

さらにQをGの p- シロー部分群とすれば，$|Q|=|a^{-1}Pa|$ より $Q=a^{-1}Pa$ となり（3）が成り立つ．□

つぎの定理も置換表現によりえられる群の一般的性質である．

定理 6.9 位数が $2n$ で n が奇数である群は，位数 n の正規部分群をもつ．

［**証 明**］ Gを位数が $2n$ で n が奇数の群とする．Gを正則表現により $(G, G/1)$ として考えるとき，Gは次数 $2n$ の置換群である．群Gは定理 6.7（1）より位数 2 の元 a をもち，注 6.4 より a は $G/1$ 上固定点をもたない．したがって a の巡回表示は n 個の互換よりなる．ここで n は奇数だから a は奇置換である．よって定理 3.6 よりGの偶置換全体の集合はGの指数 2 の，したがって位数 n の正規部分群となる．□

つぎに対称群に関する置換表現を述べるが，特に注 6.10（2）の S_6 の 6 次の置換表現は，S_6 の内部自己同型でない自己同型で，このことは§13 で自己同型群を求めるときに用いられる．

注 6.10 （1） 5 次対称群 S_5 は次数 6 の忠実な置換表現をもつ．

（2） 6 次対称群 S_6 の（1）の S_5 に同型な 6 次の部分群による置換表現は，

S_6 の自己同型であるが，S_6の互換はこの置換表現において，(2, 2, 2) 型の置換に表現される．

［証 明］ (1) G を $\{1,2,3,4,5\}$ の上の対称群 S_5 とする．Gは 6 個の 5- シロー部分群

$$P_1=\langle(1\ \ 2\ \ 3\ \ 4\ \ 5)\rangle,\qquad P_2=\langle(1\ \ 2\ \ 3\ \ 5\ \ 4)\rangle,$$
$$P_3=\langle(1\ \ 2\ \ 4\ \ 5\ \ 3)\rangle,\qquad P_4=\langle(1\ \ 2\ \ 5\ \ 4\ \ 3)\rangle,$$
$$P_5=\langle(1\ \ 2\ \ 5\ \ 3\ \ 4)\rangle,\qquad P_6=\langle(1\ \ 2\ \ 4\ \ 3\ \ 5)\rangle$$

をもつ．定理 6.7 (2) より $P_1,P_2,\cdots,P_6$ は互いにGで共役である．したがって系 6.6 より $\Omega=\{P_1,P_2,\cdots,P_6\}$ 上の置換群 $\bar{G}=\{\bar{x}\mid x\in G\}$，$\bar{x}=\begin{pmatrix}P_1 & P_2 & \cdots & P_6\\ P_1{}^x & P_2{}^x & \cdots & P_6{}^x\end{pmatrix}$ をうる．ここで $\bar{G}$ はGの部分群 $N_G(P_1)$ による置換表現によりえられたもので $N_G(P_1)=\langle(1\ \ 2\ \ 3\ \ 4\ \ 5),(2\ \ 3\ \ 5\ \ 4)\rangle$，$|N_G(P_1)|=20$ である．また表現の核は定理 6.5 より $\bigcap_{x\in G}N_G(P_1)^x$ でその位数は 20 以下である．一方補題 3.11 (1) より S_5 の正規部分群は，$S_5, A_5, 1$ で $\bigcap_{x\in G}N_G(P_1)^x\leqq S_5$ であるから，$\bigcap_{x\in G}N_G(P_1)^x=1$ である．したがって $\bar{G}$ はGに同型である．以上より S_5 は次数 6 の忠実な置換表現をもつ．

$\bar{G}$ は $\{1,2,\cdots,6\}$ 上の置換群としてつぎの性質をもつ．$G=\langle(1\ 2\ 3\ 4\ 5),(4\ 5)\rangle$ で，この 2 つのGの生成元は $\bar{G}$ の元として $\overline{(1\ 2\ 3\ 4\ 5)}=(P_1)(P_2\ P_3\ P_4\ P_5\ P_6)$，$\overline{(4\ 5)}=(P_1\ P_2)(P_3\ P_4)(P_5\ P_6)$ である．ここで P_i を i とおくと，$\bar{G}=\langle(2\ 3\ 4\ 5\ 6),(1\ 2)(3\ 4)(5\ 6)\rangle$ である．

またGの互換はすべて (4 5) と共役であるから，Gの互換は $\bar{G}$ では (2, 2, 2) 型の置換となる．

つぎに $\overline{(2\ 3\ 4\ 5)}=(P_1\ P_4\ P_6\ P_3)(P_2)(P_5)$ で，$|G|=5!=6\cdot5\cdot4$ より $\bar{G}$ は $\{1,2,\cdots,6\}$ の上で 3 重可移で，2 点の安定化群は位数 4 の巡回群である．

(2) Gを $\{1,2,\cdots,6\}$ 上の対称群 S_6，(1) による S_5 に同型な 6 次の置換群を，$H=\langle(2\ 3\ 4\ 5\ 6),(1\ 2)(3\ 4)(5\ 6)\rangle$ とする．H における 3 点の安定化群は 1 であるから，$(1\ i)\notin H$，$(1\ i)(1\ j)=(1\ i\ j)\notin H$ $(i,j=2,3,\cdots,6,i\neq j)$ となり，H によるGの左分解は

$$G=H+H(1\ 2)+H(1\ 3)+H(1\ 4)+H(1\ 5)+H(1\ 6)$$

である．$H_1=H,H_i=H(1\ i)$ $(i=2,3,\cdots,6)$ とおく．

GのHによる置換表現によりえられる群をG^*とおく．補題 3.11 (1) よりGの正規部分群は，S_6，A_6 または 1 であるから，この表現は忠実で，群としてGとG^*は同型で

あり，したがってG^*も6次の対称群 S_6 である．

一方 $(1\ 2)\in G$ に対応する $(1\ 2)^*\in G^*$ は

$$(1\ 2)^*=(H_1\ H_2)(H_3\ H_6)(H_4\ H_5)$$

となり，Gの互換はすべて $(1\ 2)$ と共役であるから，Gの互換は，G^* では $(2, 2, 2)$ 型の置換となる．□

注 6.11 （1） $n\neq 4$ のとき，n次対称群 S_n は指数 $m\,(2<m<n)$ の部分群をもたない．したがってm次の置換群として置換表現されない．

（2） 4次対称群は指数3の部分群をもち，したがって3次の置換群として置換表現される．

［証 明］ （1） $n\neq 4$ とする．S_n が指数 $m(2<m<n)$ の部分群Hをもつとする．このとき S_n の部分群Hによる置換表現をφとする．$S_n{}^\varphi$ はm次置換群で，$m<n$ より $\ker\varphi\neq 1$ である．したがって補題 3.11（1）より $\ker\varphi=A_n$ となり，$|S_n:A_n|=2$ より $2<m$ に反する．

（2） S_4 において 2- シロー部分群は，指数3の部分群である．□

問 6.1 Gを対称群S_4とし，Gの部分群 H,K を $H=\langle(1\ 2\ 3\ 4)\rangle$, $K=\langle(1\ 2)\cdot(3\ 4), (1\ 3)(2\ 4)\rangle$ とする．このとき $(G, G/H)$ および $(G, G/K)$ において，Gの元$(1\ 2)(3\ 4)$ および $(1\ 2\ 3\ 4)$ はどのように表されるか．

問 6.2 H,K を群Gの同型な部分群とする．このとき $(G, G/H)$ と $(G, G/K)$ は同型とは限らないことを，例をあげて示せ．

問 6.3 Hを群Gの指数nの部分群とする．このときGの正規部分群Nで，$|G/N|$がnの倍数でかつ $n!$ の約数であるものが存在することを示せ．

問 6.4 GをΩ上の置換群，PをGの p- シロー部分群とする．いま $i\in\Omega$ に対して $|i^G|=p^m\cdot r$, $(p,r)=1$ であれば，$|i^P|$ は p^m の倍数であり，特に P_i が G_i の p-シロー部分群のとき，$|i^P|=p^m$ となることを示せ．

§7. 原始置換群

Ω上の置換群Gにおいて，Ω の部分集合 $\Delta(\neq\phi)$ がすべての $x\in G$ に対して，$\Delta=\Delta^x$ であるかまたは $\Delta\cap\Delta^x=\phi$ のとき，ΔをGの **非原始ブロック** (imprimitive block または単に block) という．任意の置換群に対して $\{i\}$ $(i\in\Omega)$ およびΩはつねに非原始ブロックとなるから，これらを **自明な非原

始ブロックという.

補題 7.1 (1) Δを置換群Gの非原始ブロックとすると，任意の $x\in G$ に対して Δ^x もGの非原始ブロックである.

(2) Δ, Δ' を置換群Gの非原始ブロックとすると，$\Delta\cap\Delta'(\neq\phi)$ も非原始ブロックである.

［証明］ (1) $y\in G$ に対して，$\Delta^x\cap(\Delta^x)^y\neq\phi$ とすると，$(\Delta^x\cap(\Delta^x)^y)^{x^{-1}}\neq\phi$, $\Delta\cap\Delta^{xyx^{-1}}\neq\phi$ である．ここでΔはGの非原始ブロックだから，$\Delta=\Delta^{xyx^{-1}}$ となる．これより $\Delta^x=\Delta^{xy}$ となり Δ^x もGの非原始ブロックである.

(2) $x\in G$ に対して $(\Delta\cap\Delta')\cap(\Delta\cap\Delta')^x\neq\phi$ とすると，$(\Delta\cap\Delta')\cap(\Delta^x\cap\Delta'^x)\neq\phi$, $(\Delta\cap\Delta^x)\cap(\Delta'\cap\Delta'^x)\neq\phi$ である．したがって $\Delta\cap\Delta^x\neq\phi$ で $\Delta'\cap\Delta'^x\neq\phi$ である．ここで Δ, Δ' は共にGの非原始ブロックだから，$\Delta=\Delta^x, \Delta'=\Delta'^x$ となる．これより $\Delta\cap\Delta'=(\Delta\cap\Delta')^x$ となり，$\Delta\cap\Delta'$ はGの非原始ブロックである. □

GをΩ上の可移群とし，Δ_1をGの非原始ブロックとする．このときつぎの補題7.2で示すように $\Omega=\Delta_1\cup\Delta_2\cup\cdots\cup\Delta_r$ (互いに素) で $\Delta_i=\Delta_1^{x_i}(i=2, 3, \cdots, r)$ となる $x_i\in G$ が存在する．このとき集合 $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$を，$\Delta_1$を含む$G$の**非原始系**という．各 Δ_i は補題 7.1 (1) よりGの非原始ブロックである.

補題 7.2 GをΩ上の可移群，ΔをGの非原始ブロックとする．さらにΔの集合としての安定化群 $G_{(\Delta)}=H$ とおき，HによるGの左分解を

$$G=Hx_1+Hx_2+\cdots+Hx_r, \qquad x_1=1$$

とする．このときΔを含むGの非原始系が一意的に存在し，$\{\Delta=\Delta^{x_1}, \Delta^{x_2}, \cdots, \Delta^{x_r}\}$ である.

［証明］ Gは可移であるから，$\Omega=\bigcup_{x\in G}\Delta^x=\bigcup_{i=1}^{r}(\bigcup_{x\in H}\Delta^{xx_i})=\bigcup_{i=1}^{r}\Delta^{x_i}$ である.

いま $\Delta^{x_i}\cap\Delta^{x_j}\neq\phi$ とすると $\Delta^{x_ix_j^{-1}}\cap\Delta\neq\phi$ となり，ΔはGの非原始ブロックだから $\Delta^{x_ix_j^{-1}}=\Delta$ である．これより $x_ix_j^{-1}\in H$, $Hx_i=H^{x_j}$ すなわち $x_i=x_j$ となる．以上より $\Omega=\bigcup_{i=1}^{r}\Delta^{x_i}$ (互いに素) となり，$\{\Delta, \Delta^{x_2}, \cdots, \Delta^{x_r}\}$ はΔを含む非原始系である.

任意の $x\in G$ に対して，xはある Hx_i の元であるから $\Delta^x=\Delta^{x_i}$ となり，Δを含む非原始系は一意的に $\{\Delta, \Delta^{x_2}, \cdots, \Delta^{x_r}\}$ である. □

補題 7.3 $\Gamma=\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ をGの非原始系とすると，GはΓに作用し，この作用によるΓ上の置換群は $(G, G/G_{(\Delta_1)})$ と同値である.

［証 明］ 任意の $x \in G$ に対して，補題 7.2 より $\Delta_i{}^x \in \Gamma$ $(i=1,2,\cdots,r)$ である．したがって Γ 上の置換 $x^* = \begin{pmatrix} \Delta_1 & \Delta_2 & \cdots & \Delta_r \\ \Delta_1{}^x & \Delta_2{}^x & \cdots & \Delta_r{}^x \end{pmatrix}$ が定義できる．さらに任意の $x, y \in G$ に対して，$(xy)^* = x^* y^*$ であるから G は Γ に作用する．いま $G^* = \{x^* \mid x \in G\}$ とおくと定理 6.7 より $(G^*, \Gamma) \cong (G, G/G_{(\Delta)})$ である．□

G を Ω 上の可移群とする．G の非原始ブロックが自明なもの，すなわち $\{i\}$ $(i \in \Omega)$ と Ω に限るとき，G を**原始的** (primitive) または**原始置換群**という．可移群 G が自明でない非原始ブロックをもつとき，G を**非原始的** (imprimitive) または**非原始置換群**という．ここで $\Omega = \{1\}$ の上の置換群 $\{1\}$ は原始的として扱う．

例 1. $\Omega = \{1,2,3,4\}$ 上の 4 元群 $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ は $\{1,2\}$ を（任意の $i, j (\neq) \in \Omega$ に対して $\{i, j\}$ を）非原始ブロックとする非原始置換群であり，交代群 A_4 は原始置換群である．

定 理 7.4 G を Ω 上の可移群とする．

（1） H を文字 1 の安定化群 G_1 を含む G の部分群とする．このとき 1 を含む H- 軌道 1^H は G の非原始ブロックである．

（2） 逆に Δ を文字 1 を含む G の非原始ブロックとすると，$G_{(\Delta)}$ は G_1 を含む G の部分群で，Δ は $G_{(\Delta)}$- 軌道 $1^{G(\Delta)}$ である．

（3） S を G_1 を含む G の部分群全体の集合，B を文字 1 を含む G の非原始ブロック全体の集合とする．このとき $H \in S$ と $1^H \in B$ が対応する 1 対 1 対応が S と B の間に存在する．

［証 明］ （1） $\Delta = 1^H$ とおく．$x \in G$ に対して，$\Delta \cap \Delta^x \neq \phi$ とする．$i \in \Delta \cap \Delta^x$ をとると $i \in \Delta$ より，$i = 1^{y_1}$ となる $y_1 \in H$ が存在する．また $i \in \Delta^x$ だから $i = 1^{y_2 x}$ となる $y_2 \in H$ が存在する．これより $i = 1^{y_1} = 1^{y_2 x}$，$y_2 x y_1{}^{-1} \in G_1 \leqq H$ である．ここで $y_1, y_2 \in H$ であるから $x \in H$ となり $\Delta^x = \Delta$ である．すなわち Δ は G の非原始ブロックである．

（2） 任意の $x \in G_1$ に対して，$1 \in \Delta$ より $1 \in \Delta \cap \Delta^x$ である．したがって $\Delta^x = \Delta$, $x \in G_{(\Delta)}$ となり $G_1 \leqq G_{(\Delta)}$ である．さらに任意の $i \in \Delta$ に対して，G は Ω 上可移だから，$1^y = i$ となる $y \in G$ が存在する．このとき $i \in \Delta \cap \Delta^y$, $\Delta^y = \Delta$ となり $y \in G_{(\Delta)}$ である．これより $\Delta \subseteqq 1^{G(\Delta)}$ となり，$1^{G(\Delta)} \subseteqq \Delta$ であるから $\Delta = 1^{G(\Delta)}$ である．

（3） 写像 $\varphi:S\to B$ を $H\in S$ に対して（1）より $H\mapsto 1^H$ により定義できる．任意の $\varDelta\in B$ に対して（2）より $G_{(\varDelta)}\in S, 1^{G(\varDelta)}=\varDelta$ であるから $G_{(\varDelta)}{}^{\varphi}=\varDelta$ となり φ は全射である．

つぎに $H, K\in S$ に対して，$H^{\varphi}=K^{\varphi}$ すなわち $1^H=1^K$ とする．このとき任意の $x\in H$ に対して $1^x=1^y$ となる $y\in K$ が存在する．したがって $1^{xy^{-1}}=1, xy^{-1}\in G_1\leqq K$ すなわち $x\in K$ となり $H\leqq K$ である．同様にして $K\leqq H$ となり，$H=K$ である．したがって φ は単射となり，S と B は φ により1対1に対応する．□

系 7.5　G を $\varOmega$ 上の可移群とする．$i\in\varOmega$ の安定化群 G_i が G の極大部分群であるとき，そのときに限り G は原始置換群である（一般に G の部分群 H が G の極大部分群であるとは，$H\lneqq G$ で，$H\lneqq K\lneqq G$ なる G の部分群 K が存在しないときをいう）．

［証 明］（i） G_i が G の極大部分群とする．$\varDelta$ を i を含む G の任意の非原始ブロックとする．G_i は G の極大部分群であるから，定理 7.4（2）より $G_i=G_{(\varDelta)}$ または $G_{(\varDelta)}=G$ である．すなわち $\varDelta=i^{G_i}=\{i\}$ または $\varDelta=i^G=\varOmega$ となり G は原始置換群である．

（ii） G を原始置換群とし，$G_i\lneqq H\leqq G$ である G の任意の部分群 H をとる．定理 7.4（1）より i^H は G の非原始ブロックである．ここで $G_i\lneqq H$ より $\{i\}\subsetneqq i^H$ である．さらに G は原始的であるから，i^H は G の自明な非原始ブロックとなり $i^H=\varOmega$ となる．よって H は $\varOmega$ 上可移になり，$|H|=|H_i|\cdot|\varOmega|$ である．一方 $G_i<H$ より $G_i=H_i$ である．したがって $|G|=|G_i|\cdot|\varOmega|=|H_i|\cdot|\varOmega|=|H|$ となり $G=H$ で，G_i は G の極大部分群である．□

この定理より G を一般の群，H を G の極大部分群とするとき，$(G, G/H)$ は原始置換群である．したがって極大部分群と原始置換群は密接な関係をもつ．

系 7.6　G を $\varOmega$ 上の可移群とする．$|\varOmega|$ が素数であれば G は原始的である．

［証 明］ $|G:G_i|=|\varOmega|$ は素数であるから，G_i は G の極大部分群になり，系 7.5 より G は原始的である．□

定 理 7.7　G が $\varOmega$ 上2重可移群であれば，G は原始的である．

［証 明］ $\varDelta$ を $|\varDelta|\neq 1$ である G の非原始ブロックとする．$i, j(\neq)\in\varDelta$ および任意の $j'\in\varOmega-\{i\}$ をとる．G は2重可移であるから $i^x=i,\ j^x=j'$ である $x\in G$ が存在する．このとき $i\in\varDelta\cap\varDelta^x$ で $\varDelta$ は G の非原始ブロックだから $\varDelta=\varDelta^x$ である．したがって

$j\in\Delta$ より $j'=j^x\in\Delta$ となり，$\Delta=\Omega$ である．よってGは原始的である．□

このことより原始置換群は1重可移群と2重可移群の間に位置する概念とも考えることができる．

定理 7.8 GをΩ上の可移群，NをGの正規部分群とすると，N-軌道全体の集合はGの非原始系を作る．

［証明］ 注5.2より成り立つ．□

系 7.9 GがΩ上原始置換群であれば，Gの正規部分群（$\neq 1$）はΩ上可移である．

［証明］ Gの正規部分群（$\neq 1$）が可移でないならば，定理 7.8 より自明でない非原始ブロックをGがもち仮定に反する．したがってGの正規部分群（$\neq 1$）は可移である．□

系 7.10 $|\Omega|$ が奇数のとき，Ω上の可移群Gの指数2の部分群は（存在すれば）Ω上可移である．

［証明］ NをGの指数2の部分群とすると，定理 1;2.2 より $N\triangleleft G$ である．いまNはΩ上可移でないとし，ΔをN-軌道とする．定理 7.8 よりΔはGの非原始ブロックで，$N\leqq G_{(\Delta)}\lneqq G$, $|G:N|=2$ より $N=G_{(\Delta)}$ である．したがってΔを含む非原始系は補題7.2より2個の非原始ブロックよりなる．したがって $|\Omega|=2\cdot|\Delta|$ となり $|\Omega|$ が奇数であることに反する．すなわちNはΩ上可移である．□

系 7.11 PをΩ上可移である p-群とする．いま $p\lneqq|P|$ とするとPは非原始的である．

［証明］ PはΩ上可移で $p\lneqq|P|$であるから，$p\lneqq|\Omega|$ である．定理 1;2.3 よりPの中心 $Z(P)\neq 1$ であるから，位数pの元 $a\in Z(P)$ をとる．このとき $\langle a\rangle$ は位数pのPの正規部分群で，定理7.8より $\langle a\rangle$-軌道ΔはPの非原始ブロックを作る．ここで $|\langle a\rangle|=p$ より $|\Delta|=p$ で，$|\Omega|>p$ よりΔはPの自明でない非原始ブロックである．すなわちPは非原始的である．□

定理 7.12 GをΩ上の原始置換群とする．$i\in\Omega$ の安定化群 G_i の固定点集合 $F(G_i)$ が $1\lneqq|F(G_i)|$ であれば，$G_i=1$ で $|G|=|\Omega|$ でかつ $|G|$ は素数である．

［証明］ Ω上可移だから，Witt の定理（系 5.6）より $N_G(G_i)^{F(G_i)}$ は $F(G_i)$ 上可

移である．ここで $|F(G_i)|\gneqq 1$ だから，$N_G(G_i)^{F(G_i)}\neq 1$ でしたがって $G_i \lneqq N_G(G_i)$ である．

一方 G は原始置換群だから，系 7.5 より G_i は G の極大部分群である．したがって $N_G(G_i)=G$ となり $G_i \lhd G$ である．ここで G_i は Ω 上可移でないから，系 7.9 より $G_i=1$ である．したがって $|G|=|G_i|\cdot|\Omega|=|\Omega|$ となり，$G_i=1$ は G の極大部分群であるから，$|G|$ は素数である．□

系 7.13 G を Ω 上の原始置換群とする．$G_1\neq 1$ であれば任意の $i, j(\neq)\in\Omega$ に対して $G=\langle G_i, G_j\rangle$ である．

［証 明］ $G_1\neq 1$ であるから，定理 7.12 より任意の $i\in\Omega$ に対して $F(G_i)=\{i\}$ である．したがって任意の $i,j(\neq)\in\Omega$ に対して，$G_i\neq G_j$ である．ここで G_i, G_j は系 7.5 より G の極大部分群であるから，$G=\langle G_i, G_j\rangle$ である．□

定 理 7.14 G を Ω 上の原始置換群とし，$G_1\neq 1$ とする．Δ, Γ を Ω の部分集合で $|\Omega|\neq|\Gamma|\leqq|\Delta|\neq 0$ とすると，任意の $i,j(\neq)\in\Omega$ に対して，$i^a\in\Delta$, $j^a\notin\Gamma$ となる $a\in G$ が存在する．

［証 明］ $\Gamma=\phi$ であれば明らかである．したがって $\Gamma\neq\phi$ とする．

$x\in G$ に対して，$i^x\in\Delta$ であればつねに $j^x\in\Gamma$ となる $i, j(\neq)\in\Omega$ が存在すると仮定する．$T=\{x\in G\,|\,i^x\in\Delta\}, U=\{x\in G\,|\,j^x\in\Gamma\}$ とする．任意の $x\in T$ に対して $i^x\in\Delta$ だから，仮定より $j^x\in\Gamma$ となり $x\in U$ すなわち $T\subseteqq U$ である．

$\Delta=\{i_1, i_2, \cdots, i_r\}$ とする．G は可移だから $i^{a_k}=i_k$ $(k=1, 2, \cdots, r)$ となる $a_k\in G$ が存在する．定理 4.3 より $G_ia_k=\{x\in G\,|\,i^x=i_k\}$ であるから

$$T=G_ia_1+G_ia_2+\cdots+G_ia_r$$

となり，$|T|=|G_i|\cdot|\Delta|$ である．同様に $|\Gamma|=s$ とすると，$b_1, b_2, \cdots, b_s\in G$ が存在して

$$U=G_jb_1+G_jb_2+\cdots+G_jb_s$$

となり，$|U|=|G_j|\cdot|\Gamma|$ である．ここで $|\Delta|\geqq|\Gamma|$, $|G_i|=|G_j|$ であるから $|T|\geqq|U|$ となり，したがって $T\subseteqq U$ より $T=U$ である．

このとき

$$\begin{aligned}G_iU=G_iT&=G_i(G_ia_1+G_ia_2+\cdots+G_ia_r)\\&=G_ia_1+G_ia_2+\cdots+G_ia_r=T=U\end{aligned}$$

である．同様に $G_jU=U$ である．

一方 $G_i\neq 1$ であるから，系 7.13 より $G=\langle G_i, G_j\rangle$ である．したがって $G_iU=$

$G_jU = U$ より $G = GU = \langle G_i, G_j \rangle U = U$. すなわち $\Gamma = \Omega$ になり仮定に反する. 以上より $i^a \in \Delta, j^a \notin \Gamma$ となる $a \in G$ が存在する. □

定理 7.15 GをΩ上の可移群とする. Ωの部分集合Δで, $|\Delta| \gneqq \frac{1}{2}|\Omega|$ でかつ G^Δ が Δ 上原始的になるものが存在すれば, Gは原始的である.

［証 明］ Gを非原始的とし, $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ $(r \geqq 2)$ を自明でないGの非原始系とする. いま $\Delta_i \cap \Delta \neq \phi$ である非原始ブロック Δ_i をとる. このとき明らかに $\Delta_i \cap \Delta$ は G^Δ の非原始ブロックである. 一方 G^Δ は Δ 上原始的であるから, $\Delta_i \cap \Delta = \Delta$ または $|\Delta_i \cap \Delta| = 1$ である.

$\Delta_i \cap \Delta = \Delta$ とすると $\Delta_i \supseteqq \Delta$ である. したがって $|\Delta_i| \geqq |\Delta| \gneqq \frac{1}{2}|\Omega|$, $\Delta_i = \Omega$ となり仮定に反する.

つぎに $|\Delta_i \cap \Delta| = 1$ とする. このことは $\Delta_j \cap \Delta \neq \phi$ であるすべての非原始ブロック Δ_j についても $|\Delta_j \cap \Delta| = 1$ である. したがって $r \geqq |\Delta|$ である. 一方 $|\Delta_i| \geqq 2$ より $|\Omega| = r \cdot |\Delta_i| \geqq |\Delta| \cdot 2 \gneqq |\Omega|$ となり矛盾である.

以上よりGは原始的である. □

G_1をΩ_1上の置換群, G_2をΩ_2上の置換群とし, $\Omega_1 \cap \Omega_2 = \phi$ とする. このとき群としての直積 $G_1 \times G_2$を作り, $G_1 \times G_2$の元による $\Omega_1 \cup \Omega_2$ 上の置換をつぎのように定義する. (G_1, G_2 は単に群を示し, Gの安定化群ではない).

$(a, \bar{a}) \in G_1 \times G_2$, $a \in G_1$, $\bar{a} \in G_2$に対して

$$i^{(a,\bar{a})} = \begin{cases} i^a & \text{ただし } i \in \Omega_1 \text{ のとき} \\ i^{\bar{a}} & \text{ただし } i \in \Omega_2 \text{ のとき} \end{cases}$$

このとき $G_1 \times G_2$が $\Omega_1 \cup \Omega_2$ 上の置換群になることは明らかである. これを置換群 G_1, G_2 の **直 積** といい, $G_1 \times G_2$と書く.

またΩ_1上の置換群G_1, Ω_2上の置換群G_2に対して, 直積集合$\Omega_1 \times \Omega_2$上のつぎの置換群をG_1とG_2の**レス積** (**Wreath product**) といい $G_1 \wr G_2$ と書く.

$\Omega_1 = \{1, 2, \cdots, m\}$, $\Omega_2 = \{1, 2, \cdots, n\}$ とする. $G_1 \wr G_2$ は集合としては $n(=|\Omega_2|)$ 個のG_1と1個のG_2の直積集合

$$G_1 \wr G_2 = \{(a_1, a_2, \cdots, a_n, a) \mid a_i \in G_1,\ i = 1, 2, \cdots, n,\ a \in G_2\}$$

である. また$G_1 \wr G_2$の$\Omega_1 \times \Omega_2$ の上への作用は, $(i, j) \in \Omega_1 \times \Omega_2$ $(i \in \Omega_1, j \in \Omega_2)$ に対して

$$(i,j)^{(a_1,a_2,\cdots,a_n,a)} = (i^{a_j}, j^a)$$

により定義する（すなわち (i,j) の i に対しては $(a_1, a_2, \cdots, a_n, a)$ の前から j 番目の直積成分 a_j が作用する).

注 7.16 $G_1 \wr G_2$ は位数 $|G_1|^n \cdot |G_2|$ $(|\Omega_2|=n)$ の $\Omega_1 \times \Omega_2$ 上の置換群で，2元の積は

$$(a_1, a_2, \cdots, a_n, a)(b_1, b_2, \cdots, b_n, b) = (a_1 b_{1^a}, a_2 b_{2^a}, \cdots, a_n b_{n^a}, ab)$$

である（積の i 番目の成分 $a_i b_{i^a}$ は $(a_1, a_2, \cdots, a_n, a)$ の i 番目の成分 a_i と $(b_1, b_2, \cdots, b_n, b)$ の i^a 番目の成分 b_{i^a} との積である).

［証 明］（i） $G_1 \wr G_2$ の元は $\Omega_1 \times \Omega_2$ 上の置換である：

$(i,j), (i', j') \in \Omega_1 \times \Omega_2$ に対して，$(a_1, a_2, \cdots, a_n, a) \in G_1 \wr G_2$ が

$$(i,j)^{(a_1,a_2,\cdots,a_n,a)} = (i',j')^{(a_1,a_2,\cdots,a_n,a)}$$

とすると，$(i^{a_j}, j^a) = (i'^{a_{j'}}, j'^a)$ である．したがって $j^a = j'^a, j = j'$ である．これより $i^{a_j} = i'^{a_{j'}} = i'^{a_j}, i = i'$ である．すなわち $(i,j) = (i', j')$ となり $(a_1, a_2, \cdots, a_n, a)$ は $\Omega_1 \times \Omega_2$ 上の置換である．

（ii） $G_1 \wr G_2$ の異なる元は $\Omega_1 \times \Omega_2$ 上の置換としても異なる：

$(a_1, a_2, \cdots, a_n, a), (b_1, b_2, \cdots, b_n, b) \in G_1 \wr G_2$ が任意の $(i,j) \in \Omega_1 \times \Omega_2$ に対して

$$(i,j)^{(a_1,a_2,\cdots,a_n,a)} = (i,j)^{(b_1,b_2,\cdots,b_n,b)}$$

とすると，$(i^{a_j}, j^a) = (i^{b_j}, j^b)$ である．このときすべての $i \in \Omega_1$ に対して $i^{a_j} = i^{b_j}$ だから $a_j = b_j$ である．さらに j は Ω_2 の任意の文字だから，$a_j = b_j$ $(j = 1, 2, \cdots, n)$ が成り立ち，$j^a = j^b$ より $a = b$ となる．以上より $(a_1, a_2, \cdots, a_n, a) = (b_1, b_2, \cdots, b_n, b)$ である．

（iii） 任意の $(a_1, a_2, \cdots, a_n, a), (b_1, b_2, \cdots, b_n, b) \in G_1 \wr G_2$ および任意の $(i,j) \in \Omega_1 \times \Omega_2$ に対して

$$\begin{aligned}(i,j)&^{(a_1,a_2,\cdots,a_n,a)(b_1,b_2,\cdots,b_n,b)} \\ &= (i^{a_j}, j^a)^{(b_1,b_2,\cdots,b_n,b)} = (i^{a_j b_{j^a}}, j^{ab}) = (i,j)^{(\cdots,a_j b_{j^a},\cdots,ab)}\end{aligned}$$

で，$(\cdots, a_j b_{j^a}, \cdots, ab)$ は j 番目の成分が $a_j b_{j^a}$, $n+1$ 番目の成分が ab である $G_1 \wr G_2$ の元である．ここで (i,j) は $\Omega_1 \times \Omega_2$ の任意の文字であるから

$$(a_1, a_2, \cdots, a_n, a)(b_1, b_2, \cdots, b_n, b) = (a_1 b_{1^a}, a_2 b_{2^a}, \cdots, a_n b_{n^a}, ab) \in G_1 \wr G_2$$

となる．以上より $G_1 \wr G_2$ は $\Omega_1 \times \Omega_2$ 上の置換群で，位数は $|G_1|^n \cdot |G_2|$ である．□

ここで $G_1 \wr G_2$ の単位元は $(1, 1, \cdots, 1, 1')$ で 1 はG_1の単位元，$1'$ は G_2 の単

位元である．また$(a_1, a_2, \cdots, a_n, a)$ の逆元は $((a_1{}^{a^{-1}})^{-1}, (a_2{}^{a^{-1}})^{-1}, \cdots, (a_n{}^{a^{-1}})^{-1}, a^{-1})$ である．

一般の群 G_1, G_2 のレス積はつぎのようにして定義される．$G_2=\{x_1, x_2, \cdots, x_n\}$ とし，G_2 の左正則表現をとる．

$$^*G_2=\left\{{}^*a \,\middle|\, {}^*a=\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ a^{-1}x_1 & a^{-1}x_2 & \cdots & a^{-1}x_n \end{pmatrix},\ a\in G_2\right\}$$

ここで x_i を i とおきかえることにより，$^*G_2$ は $\{1, 2, \cdots, n\}$ 上の置換群になる．このとき　$G_1 \wr G_2=\{(a_1, a_2, \cdots, a_n, a)\,|\,a_i\in G, i=1, 2, \cdots, n, a\in G_2\}$　とおき，$G_1 \wr G_2$ の元の積を

$$(a_1, a_2, \cdots, a_n, a)(b_1, b_2, \cdots, b_n, b)=(a_1b_1{}^{*a}, a_2b_2{}^{*a}, \cdots, a_nb_n{}^{*a}, ab)$$

と定義することにより，$G_1 \wr G_2$ は群になる．これをG_1 とG_2 のレス積という．

定 理 7.17　$\Omega=\Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_r$（互いに素）で$|\Delta_1|=|\Delta_2|=\cdots=|\Delta_r|=m$ とする．このとき $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ を非原始系とするΩ上の非原始置換群はすべて $S_m \wr S_r$ に同値なΩ上の非原始置換群の部分群である．

［**証 明**］ $\Delta=\{1, 2, \cdots, m\}, \Gamma=\{1, 2, \cdots, r\}$ とおき，Δ上の対称群 S_m と Γ 上の対称群 S_r により $\Delta\times\Gamma$ 上のレス積 $S_m \wr S_r$ を作る．一方Ωの部分集合 Δ_j に対して $\Delta_j=\{1_j, 2_j, \cdots, m_j\}(j=1, 2, \cdots, r)$ とする．いま $\Delta\times\Gamma$ の文字 (i, j)と Ωの文字 i_j を対応させると $\Delta\times\Gamma$ とΩの間に1対1の対応がつく．そこで (i, j) と i_j を同一視すると $S_m \wr S_r$ はΩ上の置換群となり，任意の $i_j\in\Omega$，任意の $(a_1, a_2, \cdots, a_r, a)$ に対して $i_j{}^{(a_1, a_2, \cdots, a_r, a)}=i^{a_j}{}_{j^a}$ である．

したがって任意の Δ_j に対して $\Delta_j{}^{(a_1, a_2, \cdots, a_r, a)}=\Delta_j{}^a$ となり，$S_m \wr S_r$ は $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ を非原始系とする非原始置換群である．

Gを $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ を非原始系とする任意の非原始置換群とする．任意の $x\in G$ に対して，補題 7.3 よりxは $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ 上の置換を導き，$x=\begin{pmatrix} \Delta_1 & \Delta_2 & \cdots & \Delta_r \\ \Delta_{1'} & \Delta_{2'} & \cdots & \Delta_{r'} \end{pmatrix}$のとき $x'=\begin{pmatrix} 1 & 2 & \cdots & r \\ 1' & 2' & \cdots & r' \end{pmatrix}$とおくと$x'$は$S_r$ の元である．つぎに $\Delta_j{}^x=\Delta_{j'}$ において$(i_j)^x=i''_{j'}$ $(i, i''=1, 2, \cdots, m)$ とする．このとき $x_j=\begin{pmatrix} 1 & 2 & \cdots & m \\ 1'' & 2'' & \cdots & m'' \end{pmatrix}$ とおく．すると任意の $i_j\in\Omega$ に対して $(i_j)^x=i_j{}^{(x_1, x_2, \cdots, x_r, x')}$ となり，$x=(x_1, x_2, \cdots, x_r, x')$ である．したがってGは $S_m \wr S_r$ の部分群である．□

系 7.18　$\Omega=\{1, 2, \cdots, n\}$ 上の置換 a を巡回表示したとき，r_i- 巡回置換が m_i 個である巡回成分よりなるとする．ただし $i=1, 2, \cdots, t$,　$r_1>r_2>\cdots>r_t$,

$\sum_{i=1}^{t} m_i r_i = n$ とする．このとき対称群 S_n における a の中心化群 $C_{S_n}(a)$ は

$$(\langle a_1\rangle \wr S_{m_1}) \times (\langle a_2\rangle \wr S_{m_2}) \times \cdots \times (\langle a_t\rangle \wr S_{m_t})$$

に同値な置換群である．ここで a_i $(i=1, 2, \cdots, t)$ は $\{1, 2, \cdots, r_i\}$ 上の巡回置換 $(1\ 2\ \cdots\ r_i)$ である．

［証 明］ a における m_i 個の r_i－巡回置換の積よりなる置換を $a^{(i)}$ とおくと，$a=a^{(1)}a^{(2)}\cdots a^{(t)}$ である．$C_{S_n}(a)$ の元は各 $a^{(i)}$ を作る文字を集合として固定し，かつ $a^{(i)}$ と可換であり，逆に各 $a^{(i)}$ と可換である元は $C_{S_n}(a)$ の元であるから

$$C_{S_n}(a) = C_{S_{m_1r_1}}(a^{(1)}) \times C_{S_{m_2r_2}}(a^{(2)}) \times \cdots \times C_{S_{m_tr_t}}(a^{(t)})$$

である．したがって上式の各直積因子を求めればよい．

すなわち a をその巡回表示が r－巡回置換 m 個よりなる Ω 上の置換で，$|\Omega| = mr$ として $C_{S_{mr}}(a)$ を求める．

$$a = (1_1\ 2_1\ \cdots\ r_1)(1_2\ 2_2\ \cdots\ r_2)\cdots(1_m\ 2_m\ \cdots\ r_m)$$

とする．$C_{S_{mr}}(a)$ の元は a の巡回成分の間の置換をおこなうから，$C_{S_{mr}}(a)$ は $\{1_1, 2_1, \cdots, r_1\}, \{1_2, 2_2, \cdots, r_2\}, \cdots, \{1_m, 2_m, \cdots, r_m\}$ を非原始系とする非原始置換群である．いま定理 7.17 の証明におけるように，$S_r \wr S_m$ を mr 個の文字よりなる $\Omega = \{1_1, 2_1, \cdots, r_m\}$ 上の置換群とみなして，定理 7.17 より $C_{S_{mr}}(a) \leqq S_r \wr S_m$ としてよい．ここで定理 7.17 の証明におけるように，$C_{S_{mr}}(a)$ の元 x を $S_r \wr S_m$ の元 $(x_1, x_2, \cdots, x_m, x')$ と，つぎにより同一視することができる．$i_j \in \Omega$ $(i=1, 2, \cdots, r,\ j=1, 2, \cdots, m)$ に対して，$(i_j)^x = i'_{j'}$ のとき $i^{x_j} = i', j^{x'} = j'$ である．したがって，$(x_1, x_2, \cdots, x_m, x') \in S_r \wr S_m$ が

$$(1_{j^{x'}}\ 2_{j^{x'}}\ \cdots\ r_{j^{x'}}) = (1^{x_j}{}_{j^{x'}}\ 2^{x_j}{}_{j^{x'}}\ \cdots\ r^{x_j}{}_{j^{x'}}) \qquad (j=1, 2, \cdots, m)$$

が成り立つとき，そのときに限り $(x_1, x_2, \cdots, x_m, x') \in C_{S_{mr}}(a)$ である．これより x_j は $\{1, 2, \cdots, r\}$ 上の置換として $(1\ 2\ \cdots\ r)^{x_j} = (1^{x_j}\ 2^{x_j}\ \cdots\ r^{x_j}) = (1\ 2\ \cdots\ r)$ となり，$x_j \in C_{S_r}((1\ 2\ \cdots\ r))$ である．いま $\bar{a} = (1\ 2\ \cdots\ r)$ とおくと $\langle\bar{a}\rangle \leqq C_{S_r}(\bar{a})$ である．$C_{S_r}(\bar{a})$ における文字 1 の安定化群を H とおく．任意の $y \in H$ に対して，$\langle\bar{a}\rangle$ の各元は y と可換であるから，$F(y)$ を $\langle\bar{a}\rangle$ は固定する．ここで $1 \in F(y)$ で $\langle\bar{a}\rangle$ は $\{1, 2, \cdots, r\}$ 上可移であるから，$\{1, 2, \cdots, r\} \subseteqq F(y)$ となり $y=1$，すなわち $H=1$ である．したがって $C_{S_r}(\bar{a}) = \langle\bar{a}\rangle$ となり，$\langle x_j\rangle = \langle\bar{a}\rangle$ である．以上より $C_{S_{mr}}(a) = \langle\bar{a}\rangle \wr S_m$ である．□

問 7.1　次数 4 の原始置換群を求めよ．

問 7.2　次数 5 の原始置換群を求めよ．

問 7.3　G を Ω 上の可移群とし，G_1 の軌道を $\Delta_1(1) = \{1\}, \Delta_2(1), \cdots, \Delta_r(1)$ とする．

(1)　任意の $i \in \Omega$ に対して，$1^x = 1^{x'} = i$ のとき $\Delta_s(1)^x = \Delta_s(1)^{x'}$ で，したがっ

て G_i の軌道は $\Delta_1(i)=\{i\}, \Delta_2(i), \cdots, \Delta_r(i), \Delta_s(i)=\Delta_s(1)^{a_i}$ $(s=2,3,\cdots,r)$, $1^{a_i}=i$ であることを示せ.

（2） $i,j\in\Omega$ に対して, Ωに適当なm個の点 $i_1,i_2,\cdots,i_m$ が存在して,

$$\Delta_s(i)\cap\Delta_s(i_1)\neq\phi,\quad \Delta_s(i_1)\cap\Delta_s(i_2)\neq\phi,\quad \cdots,\quad \Delta_s(i_m)\cap\Delta_s(j)\neq\phi$$

のとき, i と j は Δ_s により結ばれているということにする.

（i） Ωの任意の点 i および任意の Δ_s $(s=2,3,\cdots,r)$ に対して, 1 と i が Δ_s により結ばれているならば, Gは原始置換群であることを示せ.

（ii） 逆にGを $G_1\neq 1$ である原始置換群とする. このとき任意のΩの2点 i,j および任意の Δ_s $(s=2,3,\cdots,r)$ に対して, i と j は Δ_s で結ばれていることを示せ.

§8. 多重可移群

多重可移群の例としては, §3 で述べたようにn次対称群はn重可移であり, n次交代群は $(n-2)$ 重可移である. また2重, 3重可移群の例としては§10で述べる射影線形群がある. しかし4重, 5重可移群については対称群, 交代群以外には第3章で述べる4個の Mathieu 群しか知られていないし, これ以外には存在しないのではないかと思われている.

定理 8.1 (Jordan) GをΩ上の原始置換群, Δを$1\leqq|\Delta|\lneqq|\Omega|-1$である$\Omega$の部分集合とする.

（1） G_Δ が $\Omega-\Delta$ 上可移であれば, GはΩ上2重可移である.

（2） G_Δ が $\Omega-\Delta$ 上原始的であれば, GはΩ上 $(|\Delta|+1)$ 重可移である.

［証 明］ $\Gamma=\Omega-\Delta$ とおく. 仮定より G_Δ はΓ上可移である.

$|\Delta|\gneqq 1$ のとき, 適当な元 $a\in G$ により $\bar{\Delta}=\Delta\cap\Delta^a$ とおくと, $1\leqq|\bar{\Delta}|\lneqq|\Delta|$, $|\Gamma\cap\Gamma^a|\neq 0$ かつ $G_{\bar{\Delta}}$ は $\Omega-\bar{\Delta}$ 上可移になることを示す.

$|\Delta|\lneqq\frac{1}{2}|\Omega|$ とする. Gは原始的で $1\lneqq|\Delta|\lneqq|\Omega|$ だからΔはGの非原始ブロックではない. したがって $\Delta\neq\Delta^a$ かつ $\Delta\cap\Delta^a\neq\phi$ となるGの元aが存在する. このとき $\bar{\Delta}=\Delta\cap\Delta^a$ とおくと $1\leqq|\bar{\Delta}|\lneqq|\Delta|$である. また $|\Gamma|\gneqq\frac{1}{2}|\Omega|$ より $|\Gamma\cap\Gamma^a|\neq 0$ である.

つぎに $|\Delta|\geqq\frac{1}{2}|\Omega|$ とする. $1\lneqq|\Omega-\Delta|=|\Gamma|\lneqq|\Omega|$ より上のΔの場合と同様に, $\Gamma\neq\Gamma^a$ かつ $\Gamma\cap\Gamma^a\neq\phi$ となる $a\in G$ が存在する. $\Gamma\neq\Gamma^a$ より $\Delta\neq\Delta^a$ である. したがって $|\bar{\Delta}|=|\Delta\cap\Delta^a|\lneqq|\Delta|$ である. また $\Gamma\cap\Gamma^a\neq\phi$ で $|\Gamma|\leqq\frac{1}{2}|\Omega|$ だから $|\bar{\Delta}|=|\Delta\cap\Delta^a|\geqq 1$ である.

以上より $1 \leqq |\bar{\Delta}| \lneqq |\Delta|$, $|\Gamma \cap \Gamma^a| \neq 0$ をみたす元 a が存在する．さらにG_ΔはΓ上可移だから，G_{Δ^a} は Γ^a 上可移で，したがって $\Gamma \cap \Gamma^a \neq \phi$ より $\langle G_\Delta, G_{\Delta^a} \rangle$ は $\bar{\Delta} = \Delta \cap \Delta^a$ を点毎に固定し $\Gamma \cup \Gamma^a$ 上可移となる．ここで $\Omega - \bar{\Delta} = \Gamma \cup \Gamma^a$ であるから $G_{\bar{\Delta}}$ は $\Omega - \bar{\Delta}$ 上可移である．この性質を用いて (1), (2) を証明する．

（1） G_Δ が $\Omega - \Delta$ 上可移になる Ω の部分集合 Δ $(\neq \phi)$ のうち長さが最小になる Δ をとる．$|\Delta| \gneqq 1$ であれば上に示した $\bar{\Delta}$ が存在するから $|\Delta| = 1$ である．したがってGはΩ上2重可移である．

（2） G_Δ は $\Omega - \Delta$ 上原始的とする．（1）よりGは2重可移である．したがって $|\Delta| = 1$ のときは成立しているから，$|\Delta| > 1$ とする．このとき $i \in \Delta$ に対して G_i が $\Omega - \{i\}$ 上原始的であれば，帰納法を用いて $\Omega - \{i\}$ 上の置換群として G_i は $((|\Delta| - 1) + 1)$ 重可移となり，これよりGはΩ上 $(|\Delta| + 1)$ 重可移になる．したがって以下 G_i が $\Omega - \{i\}$ 上原始的になることを示す．

G_Δ が $\Omega - \Delta$ 上原始的になる Ω の部分集合$(\neq \phi)$のうち長さが最小になる Δ をとる．$|\Delta| > 1$ とすると上で示した $a \in G$ が存在して，$\bar{\Delta} = \Delta \cap \Delta^a$ に対して $G_{\bar{\Delta}}$ は $\Omega - \bar{\Delta}$ 上可移で，$1 \leqq |\bar{\Delta}| \lneqq |\Delta|$ である．ここで $\Omega - \bar{\Delta} = \Gamma \cup \Gamma^a$ であり，$\Gamma \cup \Gamma^a \neq \phi$ より $|\Gamma| \gneqq \frac{1}{2}|\Gamma \cup \Gamma^a|$ である．したがって $G_{\bar{\Delta}}$ は $\Gamma \cup \Gamma^a$ 上可移で，$G_{\bar{\Delta}}$ の部分群 G_Δ は Γ 上原始的かつ $|\Gamma| \gneqq \frac{1}{2}|\Gamma \cup \Gamma^a|$ となり，定理 7.15 より $G_{\bar{\Delta}}$ は $\Gamma \cup \Gamma^a$ 上原始的になる．このことは $|\Delta|$ の最小性に反し，したがって $|\Delta| = 1$ である．すなわち $\Delta = \{i\}$ で G_i は $\Omega - \{i\}$ 上原始的になる．以上により（2）は証明された．□

補題 8.2 G がΩ上 $(|\Omega| - 2)$ 重可移置換群 $(|\Omega| \geqq 3)$ であれば，G は対称群 S^Ω または交代群 A^Ω である．

［**証明**］ 異なる任意の3文字 $i, j, k \in \Omega$ をとり，$\Delta = \Omega - \{i, j, k\}$ とおく．G は $(|\Omega| - 2)$ 重可移で，$|\Delta| = |\Omega| - 3$ であるから，G_Δ は $\{i, j, k\}$ 上可移である．したがってGは 3-巡回置換$(i\ j\ k)$をもち，補題 3.10 より $G = S^\Omega$ または A^Ω である．□

系 8.3 GをΩ上の原始置換群とする．

（1） Gが互換をもてば，Gは対称群 S^Ω である．

（2） Gが3-巡回置換をもてば，Gは対称群 S^Ω または交代群 A^Ω である．

（3） pを素数とする．$|\Omega| \geqq p + 3$ でGが p-巡回置換をもてば，Gは対称群 S^Ω または交代群 A^Ω である．

［**証明**］ （1） Gの互換を $(i\ j)$ とし $\Delta = \Omega - \{i, j\}$ とおくと，G_Δ は $\Omega - \Delta = \{i, j\}$

上原始的である．したがって定理 8.1（2）よりGはΩ上$(|\Omega|-1)$重可移になり，補題8.2より$G \geqq A^{\Omega}$であるが，奇置換$(i\ j)$をもつから$G=S^{\Omega}$である．

（2）Gは（1）と同様に$(|\Omega|-2)$重可移になり，補題 8.2 よりS^{Ω}またはA^{Ω}である．

（3）$a \in G$をp-巡回置換とし，$F(a)=\{1, 2, \cdots, t\}$, $a=(t+1\ t+2\ \cdots\ n)$ $(n=t+p)$とする．このとき$|\{t+1, t+2, \cdots, n\}|$は素数であるから，系7.6より$G_{F(a)}$は$\Omega-F(a)$上原始的である．したがって定理 8.1（2）より$G$は$t+1$重可移である．$P=\langle a\rangle$とおく．$P$は$G_{1 2 \cdots t}$の$p$-シロー部分群で，$G_{1 2 \cdots t}$の$p$-シロー部分群は定理6.7（2）よりすべて$G_{1 2 \cdots t}$-共役であるから，系5.6より$N_G(P)^{F(P)}$は$F(P)$上$t$重可移である．ここで$|F(P)|=t$だから$N_G(P)^{F(P)}$は$F(P)$上対称群である．さらに定理 1;3.5 より$N_G(P)/C_G(P)$は$P$の自己同型群とみなせるから，定理 1;3.4 より可換群である．したがって$N_G(P)^{F(P)}/C_G(P)^{F(P)}$は$N_G(P)/C_G(P)$の準同型像として可換群となり，補題 3.11 より$C_G(P)^{F(P)}$は$F(P)$上の交代群を含む．

$|P|=2,3$のときは(1),(2)より成り立つ．したがって$|P| \gneqq 3$とする．$|F(P)|=t \geqq 3$で$C_G(P)^{F(P)} \geqq A_t$より，$C_G(P)$は位数が3のべきで$F(P)$上3-巡回置換である元　$x=(1\ 2\ 3)(4)\cdots(t)\cdots$　をもつ．このとき$|\{t+1,\ t+2, \cdots, n\}|=p \neq 3$より$\{t+1,\ t+2, \cdots,\ n\}$上に$x$は固定点$i$をもつ．$x$と$P$の各元は可換であるから$P$は$F(x)$を固定し，さらに$P$は$\{t+1, t+2, \cdots,\ n\}$上可移であるから，$i^P=\{t+1,\ t+2, \cdots, n\} \subseteqq F(x)$となり，$x=(1\ 2\ 3)$である．したがって（2）より$G$は$S^{\Omega}$または$A^{\Omega}$である．□

この系8.3でGを単に可移群としたとき，Gは必ずしも対称群にはならない．たとえばpを素数とし，$|\Omega|=p^m$ $(m \geqq 2)$とする．いまPを対称群S^{Ω}のp-シロー部分群とすると，Pはp^m-巡回置換をもつからΩ上可移であり，しかもp-巡回置換をもつ．このときPは系 7.11 より非原始的である．このように定理8.3においてGが原始的である仮定は必要である．

つぎに Witt の定理（系 5.6）の成り立つ重要な例を定理としてあげる．

定理 8.4　GをΩ上のt重可移群とし，NをGの正規部分群とするとき，$N_G(N_{1 2 \cdots t})^{F(N_{1 2 \cdots t})}$は$F(N_{1 2 \cdots t})$上$t$重可移である．

［証明］$(N_{1 2 \cdots t})^x \leqq G_{1 2 \cdots t}$である任意の元$x \in G$をとる．$N$は$G$の正規部分群であるから，補題 4.2 (2) を用いて，$(N_{1 2 \cdots t})^x=(N^x)_{1^x 2^x \cdots t^x}=N_{1^x 2^x \cdots t^x}$であ

る．したがって $N_{1^x 2^x \cdots t^x} \leqq N \cap G_{1\,2\cdots t} = N_{1\,2\cdots t}$ で $|(N_{1\,2\cdots t})^x| = |N_{1\,2\cdots t}|$ であるから，$(N_{1\,2\cdots t})^x = N_{1\,2\cdots t}$ である．これより $N_{1\,2\cdots t}$ は $G_{1\,2\cdots t}$ の部分群として系 5.6 の仮定をみたし，$N_G(N_{1\,2\cdots t})^{F(N_{1\,2\cdots t})}$ は $F(N_{1\,2\cdots t})$ 上 t 重可移である．□

定理 8.5　GをΩ上の t 重可移群，NをGの正規部分群，P を $N_{1\,2\cdots t}$ の p-シロー部分群とすると，$N_G(P)^{F(P)}$ は $F(P)$ 上 t 重可移である．

［証明］ $P^x \leqq G_{1\,2\cdots t}$ である任意の元 $x \in G$ をとる．$N \trianglelefteq G$ より，$P^x \leqq N \cap G_{1\,2\cdots t} = N_{1\,2\cdots t}$ である．したがって定理 6.7 (2) より $y \in N_{1\,2\cdots t} \leqq G_{1\,2\cdots t}$ が存在して，$P^x = P^y$ である．よって系 5.6 より $N_G(P)^{F(P)}$ は $F(P)$ 上 t 重可移である．□

与えられた置換群の可移度を決定するのは，なかなか困難であるが，つぎの定理は Witt の定理と共に可移度を決める上で重要な役割をはたす．

定理 8.6　(Livingstone, Wagner) GをΩ上の置換群，pを素数とする．Ω の任意の異なる t 個の点に対して，ちょうどこの t 個の点を固定する G の p-部分群 ($\neq 1$) が存在すれば，GはΩ上 t 重可移である．

［証明］ $i_1, i_2, \cdots, i_{t-1}$ をΩの任意の異なる $t-1$ 個の点とし，$\Delta = \Omega - \{i_1, i_2, \cdots, i_{t-1}\}$ とおく．$G_{i_1 i_2 \cdots i_{t-1}}$ は仮定よりΔのちょうど 1 点を固定する p-部分群 $P(\neq 1)$ をもつ．このときΔ上の P-軌道は長さ 1 のもの 1 個と他はすべてpの倍数の長さをもち，$G_{i_1 i_2 \cdots i_{t-1}}$-軌道はこれら P-軌道の和集合からなる．

いま $G_{i_1 i_2 \cdots i_{t-1}}$ はΔ上可移でないとする．すると長さがpの倍数である $G_{i_1 i_2 \cdots i_{t-1}}$-軌道$\Gamma$が$\Delta$に存在する．$i \in \Gamma$ に対して，仮定よりちょうど t 個の点 $i_1, i_2, \cdots, i_{t-1}, i$ を固定する p-部分群 $R(\neq 1)$ が存在する．$R \leqq G_{i_1 i_2 \cdots i_{t-1}}$ よりΓをRは固定する．このとき $i \in \Gamma$ よりΓは長さ 1 の R-軌道 1 個といくつかの長さがpの倍数である R-軌道からなり，Γの長さがpの倍数であることに反する．したがって $G_{i_1 i_2 \cdots i_{t-1}}$ はΔ上可移である．

$\Omega - \{i_1, i_2, \cdots, i_r\}$ ($0 \leqq r \leqq t-2$. ただし $r=0$ のときはΩに等しいとする) の任意の 2 点 k, l に対して，$\Omega - \{i_1, i_2, \cdots, i_r, k, l\}$ の $(t-1)-r$ 個の点 $j_{r+1}, j_{r+2}, \cdots, j_{t-1}$ をとる．このとき上で示したことより $G_{i_1 i_2 \cdots i_r j_{r+1} \cdots j_{t-1}}$ は $\Omega - \{i_1, i_2, \cdots, i_r, j_{r+1}, \cdots, j_{t-1}\}$ 上可移となり，したがってkをlに移す元をもつ．ここで $G_{i_1 i_2 \cdots i_r} \geqq G_{i_1 i_2 \cdots i_r j_{r+1} \cdots j_{t-1}}$ で k, l は $\Omega - \{i_1, i_2, \cdots, i_r\}$ の任意の 2 点であるから，$G_{i_1 i_2 \cdots i_r}$ は $\Omega - \{i_1, i_2, \cdots, i_r\}$ 上可移である．

以上より順次 $G, G_{i_1}, \ldots, G_{i_1 i_2 \cdots i_{t-1}}$ をとることによりGはΩ上 t 重可移になる．□

系 8.7 (Livingstone, Wagner) GをΩ上のt重可移群，NをGの正規部分群，Pを$N_{12\cdots t}$のp-シロー部分群とする．いまΔを$\Omega-\{1,2,\cdots,t\}$上のP-軌道のうち長さが最小のものとし，iをΔの任意の点とする．このとき$N_G(P_i)^{F(P_i)}$は$F(P_i)$上t重可移である．

［証 明］ $|\Delta|=1$のとき，すなわち$i\in F(P)$のときは$P=P_i$である．したがって定理8.5より$N_G(P)^{F(P)}$は$F(P)$上t重可移である．

$|\Delta|\geqq 1$のとき，すなわち$F(P)=\{1,2,\cdots,t\}$とする．このとき$F(P_i)\supsetneqq F(P)$で$|P_i|=|P|/|\Delta|$である．

$F(P_i)$の任意の異なるt個の点$i_1, i_2, \cdots, i_t$をとる．$N_{i_1 i_2\cdots i_t}\geqq P_i$であるから，$P_i$は$N_{i_1 i_2\cdots i_t}$のある$p$-シロー部分群$R$に含まれる．$G$は$\Omega$上$t$重可移であるから$a=\begin{pmatrix}1 & 2 & \cdots & t & \cdots\\ i_1 & i_2 & \cdots & i_t & \cdots\end{pmatrix}\in G$が存在し，$P^a$は$(N_{12\cdots t})^a=N_{i_1 i_2\cdots i_t}$の$p$-シロー部分群である．したがって定理6.7（2）より$P^{ab}=R$である$b\in N_{i_1 i_2\cdots i_t}$が存在する．これより$F(R)=\{i_1,i_2,\cdots,i_t\}$で$\Delta'=\Delta^{ab}$は$\Omega-F(R)$上の長さ最小の$R$-軌道である．いま$N_R(P_i)=\bar{R}$とおくと定理1;2.3より$\bar{R}\gneqq P_i$で$F(\bar{R})\supseteqq F(R)$である．

$F(\bar{R})\supsetneqq F(R)$とし，$i'\in F(\bar{R})-F(R)$をとる．このとき$|R_{i'}|=|R|/|i'^R|$で，$|R|=|P|$, $|i'^R|\geqq|\Delta'|=|\Delta|$より$|R_{i'}|\leqq|P_i|$である．一方$i'\in F(P_i)$であるから$R_{i'}\geqq P_i$となり，$R_{i'}=P_i$である．しかしこのことは$R_{i'}\geqq\bar{R}>P_i$に反する．

以上より$F(\bar{R})=F(R)=\{i_1, i_2, \cdots, i_t\}$である．すなわち$\bar{R}^{F(P_i)}$は$F(P_i)$のちょうど$t$個の点を固定する$p$群である．したがって定理8.6より$N_G(P)^{F(P_i)}$は$F(P_i)$上$t$重可移である．□

この定理においてP_iはt個より多くの点を固定するNのp-部分群で位数最大のものである．したがって系8.7はつぎのようにいってもよい．

系 8.7′ GをΩ上のt重可移群とし，NをGの正規部分群，Pを$|F(P)|\gneqq t$であるNのp-部分群のうち位数最大のものとする．このとき$N_G(P)^{F(P)}$は$F(P)$上t重可移である．

定理8.4において，Nをt重可移群の正規部分群と仮定した．しかしこの仮定をつぎのように弱めることにより非常に近い結果をうることができる．

定 理 8.8 (O′ Nan) GをΩ上のt重可移群，Nを$G_{12\cdots t-1}$の正規部分群とするとき，$G^{F(N_t)}$は$F(N_t)$上t重可移である．

［証 明］ $t=1$のとき，すなわちGが可移で$N\trianglelefteq G$のときは定理8.4より成り立つ．

したがって以下 $t\geqq 2$ とする.

$1,2,\cdots,t-1$ の任意の順列を $(i_1,i_2,\cdots,i_{t-1})$ とすると, $H=G_{i_1 i_2\cdots i_{t-2}}$ は $\Omega-\{i_1,i_2,\cdots,i_{t-2}\}$ 上2重可移で N は $H_{i_{t-1}}$ の正規部分群である. いま $H^{F(N_t)}$ が $F(N_t)-\{i_1,i_2,\cdots,i_{t-2}\}$ 上2重可移であれば, $i_1,i_2,\cdots,i_{t-2}$ は $1,2,\cdots,t-1$ の任意の $t-2$ 個の点であるから, $G^{F(N_t)}$ は $F(N_t)$ 上 t 重可移になる. したがって補題 8.11 を示せばよい. □

なお補題 8.11 の証明に必要な p-シロー部分群についての簡単な補題を2つ準備しておく.

補題 8.9 Nを群Gの正規部分群, PをGの p-シロー部分群とするとき, $N\cap P$ はNの p-シロー部分群である.

[証明] $N\trianglelefteq G$ であるから, NP はGの部分群であり, 定理 1;1.4により $|NP|=|N|\cdot|P|/|N\cap P|$ である. したがって $|N|/|N\cap P|=|NP|/|P|$ となる. ここでPはGの p-シロー部分群であるから, $|NP|/|P|$ はpと互いに素である. すなわち $N\cap P$ は Nにおいて指数がpと互いに素であるp群となり, したがって $N\cap P$ はNの p-シロー部分群である. □

補題 8.10 Nを群Gの正規部分群, HをGの部分群, PをHの p-シロー部分群とする. このときNの p-シロー部分群 Qで, $P\leqq N_G(Q)$ となるものが存在し, $P\cap N=P\cap Q$ でかつ $P\cap Q$ は $H\cap N$ の p-シロー部分群である.

[証明] Nの p-シロー部分群全体の集合をΩとするとき, 定理 6.7 (3) より $|\Omega|=kp+1$ である. さらに, 定理 6.7 (2) よりΩの元は共役で, NはGの正規部分群であるから, Ωは G-共役なもの全体よりなる. したがって系 6.6 におけるようにGは共役によりΩに作用する. このときPは G のp部分群として, この作用によるΩ上の P-軌道の長さはすべてpのべきである. 一方 $|\Omega|=kp+1$ であるから, P は長さ1の軌道をもつ. いま長さ1の P-軌道を作るΩの元をQとすると, $Q^P=Q$ すなわち $P\leqq N_G(Q)$ である.

$H\cap N\trianglelefteq H$ でPはHの p-シロー部分群であるから, 補題 8.9 より $P\cap(H\cap N)=P\cap N$ は $H\cap N$ の p-シロー部分群である. また $P\leqq N_G(Q)$ であるから, PQ したがって$(P\cap N)Q$ はp群である. ここで $(P\cap N)Q$ はQを含むNのp部分群で, QはNの p-シロー部分群であるから, $(P\cap N)Q=Q$, $P\cap N\leqq Q$ すなわち $P\cap N=P\cap Q$ である. □

補題 8.11 (O'Nan) GをΩ上の2重可移群，NをG_1の正規部分群とするとき，$G^{F(N_2)}$ は $F(N_2)$ 上2重可移である．

［証明］ $N=1$ のときは明らかであるから，$N \gneqq 1$ として（i）から（v）にわけて証明する．

（i） $F(N)=\{1\}$ で，任意の $i \in \Omega-\{1\}$ に対して $N_i \trianglelefteq G_{1i}$ となり，$|N_i|$ は i に関係なく一定である．

（証明） $N \trianglelefteq G_1$ より $N_i = N \cap G_{1i} \trianglelefteq G_{1i}$ である．任意の $i, j \in \Omega-\{1\}$ に対して $i^x=j$ となる元 $x \in G_1$ が存在する．このとき $N \trianglelefteq G_1$ より $(N_i)^x=(N^x)_{i^x}=N_j$ となり $|N_i|=|N_j|$ である．さらに注5.2より $\Omega-\{1\}$上の N-軌道の長さはすべて等しく，$N \neq 1$ よりその長さは1でないから，$F(N)=\{1\}$ である．

（ii） 任意の $i \in \Omega$ に対して，G_i に含まれNと共役な部分群はただ1つである．したがって $N=N^{(1)}$ とし $x \in G$ に対して $(N^{(1)})^x=N^{(1^x)}$ と書く．このとき $N^{(i)}{}_j \trianglelefteq G_{ij}$ である．

（証明） G は可移だから $N^x \leqq G_i$ $(x \in G)$ となる N^x は少なくとも1つ存在する．いま$N^x, N^y \leqq G_i$ $(x, y \in G)$ とする．（i）より$F(N^x)=F(N^y)=\{i\}$ である．ここで $F(N^x)=F(N)^x=\{1^x\}$，$F(N^y)=F(N)^y=\{1^y\}$ であるから，$1^x=1^y=i$，$1^{xy^{-1}}=1$，$xy^{-1} \in G_1$ である．したがって $N \trianglelefteq G_1$ より $N^{xy^{-1}}=N$，$N^x=N^y$ となり，G_i に含まれるNと共役な部分群はただ1つである．

（i）より $N^{(1)}{}_{i'} \trianglelefteq G_{1i'}$ でGは2重可移であるから，$a=\begin{pmatrix}1 & i' & \cdots \\ i & j & \cdots\end{pmatrix} \in G$が存在し $(N^{(1)}{}_{i'})^a \trianglelefteq (G_{1i'})^a$，$N^{(i)}{}_j \trianglelefteq G_{ij}$ である．

（iii） Pを $N^{(1)}{}_2$ の p-シロー部分群とする．任意の $i \in F(P)-\{2\}$ に対して，$P \leqq N_G(Q)$ である $N^{(2)}{}_i$ の p-シロー部分群Qが存在し，$|PQ|$ は i に関係なく $N^{(1)}{}_2 \cdot N^{(2)}{}_1$ の p-シロー部分群の位数に等しい．

（証明） （ii）より $N^{(2)}{}_i \trianglelefteq G_{2i}$ で，$P \leqq G_{2i}$ であるから補題 8.10 より，$P \leqq N_G(Q)$ となる $N^{(2)}{}_i$ の p-シロー部分群Qが存在し，$P \cap N^{(2)}{}_i = P \cap Q$ である．

$P \leqq N^{(1)}{}_2, Q \leqq N^{(2)}{}_i$ より $P \cap Q \leqq N^{(1)}{}_2 \cap N^{(2)}{}_i$ である．さらに $N^{(1)}{}_2 \trianglelefteq G_1$ より $N^{(1)}{}_2 \cap N^{(2)}{}_i \leqq G_1 \cap N^{(2)}{}_i \leqq N^{(2)}{}_1$ となり，$P \cap Q \leqq N^{(1)}{}_2 \cap N^{(2)}{}_1$ である．Pは $N^{(1)}{}_2$ の p-シロー部分群で，（ii）より $N^{(2)}{}_1 \trianglelefteq G_{12}$ であるから，補題8.10より $P \cap N^{(2)}{}_1$ は $N^{(1)}{}_2 \cap N^{(2)}{}_1$ の p-シロー部分群である．さらに $P \leqq G_i$ より $P \cap N^{(2)}{}_1 \leqq G_i \cap N^{(2)}{}_1 \leqq N^{(2)}{}_i$ であるから，$P \cap N^{(2)}{}_1 \leqq P \cap N^{(2)}{}_i = P \cap Q$ となる．ここで $P \cap N^{(2)}{}_1$ は $N^{(1)}{}_2 \cap N^{(2)}{}_1$ の p-シロー部分群であるから，$P \cap Q = P \cap N^{(2)}{}_1$ となり $P \cap Q$ は $N^{(1)}{}_2 \cap N^{(2)}{}_1$ の

p-シロー部分群である.

一方定理 1;1.4 より $|N^{(1)}{}_2N^{(2)}{}_1|=|N^{(1)}{}_2|\cdot|N^{(2)}{}_1|/|N^{(1)}{}_2\cap N^{(2)}{}_1|$ である. ここで (i), (ii) より $N^{(1)}{}_2$ と $N^{(2)}{}_1$ は共役で, したがってその p-シロー部分群の位数は $|P|$ $(=|Q|)$ である. さらに $P\cap Q$ は $N^{(1)}{}_2\cap N^{(2)}{}_1$ の p-シロー部分群であるから, $N^{(1)}{}_2N^{(2)}{}_1$ の p-シロー部分群の位数は $|P|\cdot|Q|/|P\cap Q|=|PQ|$ に等しい.

(iv) Pを $N^{(1)}{}_2$ の p-シロー部分群とする. 任意の $i\in F(P)$ に対して, i を固定する $N^{(2)}{}_1$ の p-シロー部分群が存在する.

(証明) $P\leqq N^{(2)}{}_1$ ならば, Pは $N^{(2)}{}_1$ の p-シロー部分群でもあるから (iv) は成立する.

したがって $P\not\leqq N^{(2)}{}_1$ とする. G_1 は $\Omega-\{1\}$ 上可移で, $N^{(1)}\leqq G_1$ かつPは $N^{(1)}{}_2$ の p-シロー部分群であるから, 定理 8.5 より $N_{G_1}(P)^{F(P)-\{1\}}$ は $F(P)-\{1\}$ 上可移である. いま $x\in N_G(P)$ で $x\notin G_1$ である元xが存在すれば $N_G(P)^{F(P)}$ は $F(P)$ 上2重可移となり, $N_G(P)$ は $y=(1\,2)\cdots$ なる元をもつ. このとき $P=P^y\leqq(N^{(1)}{}_2)^y=N^{(2)}{}_1$ となり仮定に反する. したがって $N_G(P)\leqq G_1$ である.

(iii) より $P\leqq N_G(Q)$ となる $N^{(2)}{}_i$ の p-シロー部分群 Q が存在し, $|PQ|$ は $N^{(1)}{}_2N^{(2)}{}_1$ の p-シロー部分群の位数に等しい. いま$1\in F(Q)$であれば, Qは $N^{(2)}{}_1$ の p-シロー部分群になり (iv) は成り立つ.

したがって $1\notin F(Q)$ として矛盾を導く. ここで $N_G(P)\leqq G_1$ であるから $Q\not\leqq N_G(P)$ である. いま $N_{PQ}(P)=R$ とおくと, $R\lneqq PQ$ で $R\leqq G_1$ である. 定理 1;2.3 より $R\lneqq N_{PQ}(R)$ であるから, $a\in N_{PQ}(R)-R$ をとると $P^a\neq P$ で, $P\leqq R$ より $P^a\leqq R$ となり, さらに P^a は $(N^{(1)}{}_2)^a=N^{(1^a)}{}_{2^a}=N^{(1^a)}{}_2$ の p-シロー部分群である. ここで $1^a\in F(R)\subseteqq F(P)$ であるが, $1^a=1$ とすると $P\lneqq PP^a\leqq N^{(1)}{}_2$ となり, Pが $N^{(1)}{}_2$ の p-シロー部分群であることに反する. したがって $1^a\neq1$ となり, $N_G(P)$ は $F(P)-\{1\}$ 上可移であるから, $(1^a)^b=2$ となる元 $b\in N_G(P)$ が存在する.

このとき P^{ab} は $(N^{(1^a)}{}_2)^b=N^{(2)}{}_{2^b}$ の p-シロー部分群で, $P^a\leqq P\cdot P^a$ より $P^{ab}\leqq P^b$. $P^{ab}=PP^{ab}$ すなわち $P\leqq N_G(P^{ab})$ である. さらに $2\in F(P)$ より $2^b\in F(P)$ である. したがって (iii) より $|PP^{ab}|$ は $N^{(1)}{}_2N^{(2)}{}_1$ の p-シロー部分群の位数に一致する. しかし $|PP^{ab}|=|PP^a|\leqq|R|\lneqq|PQ|$ で $|PQ|$ も $N^{(1)}{}_2N^{(2)}{}_1$ の p-シロー部分群の位数に等しいから, 矛盾である. 以上より $1\in F(Q)$ となり, Qは $N^{(2)}{}_1$ の p-シロー部分群で $i\in F(Q)$ である.

(v) $F(N^{(1)}{}_2)=F(N^{(2)}{}_1)$ で, $F(N^{(1)}{}_2)=\Delta$とおくと, G^Δ は Δ 上2重可移であ

る．

（証明）$|N^{(1)}{}_2|=|N^{(2)}{}_1|=p_1{}^{e_1}p_2{}^{e_2}\cdots p_r{}^{e_r}$（$p_1,p_2,\cdots,p_r$ は互いに異なる素数）とする．任意の $i\in F(N^{(1)}{}_2)$ に対して（iv）より $i\in F(P_k)$ となる $N^{(2)}{}_1$ の p_k-シロー部分群 P_k がすべての $k=1,2,\cdots,r$ に対して存在する．このとき $N^{(2)}{}_1=\langle P_1,P_2,\cdots,P_r\rangle$ であるから，$i\in F(N^{(2)}{}_1)$ である．これより $F(N^{(1)}{}_2)\subseteqq F(N^{(2)}{}_1)$ となり，$N^{(1)}{}_2$ と $N^{(2)}{}_1$ は共役であるから，$F(N^{(1)}{}_2)=F(N^{(2)}{}_1)$ である．いま $F(N^{(1)}{}_2)=\varDelta$ とおく，$\varDelta=\{1,2\}$ のとき，G は2重可移であるから，$G^{\varDelta}$ は $\varDelta$ 上2重可移である．$\varDelta\supsetneqq\{1,2\}$ のとき，定理 8.4 より $N_{G_1}(N^{(1)}{}_2)$ は $\varDelta$ を固定し，$\varDelta-\{1\}$ 上可移であり，$N_{G_2}(N^{(2)}{}_1)$ は $F(N^{(2)}{}_1)$ を固定し，$F(N^{(2)}{}_1)-\{2\}$ 上可移である．ここで $F(N^{(2)}{}_1)=\varDelta$ であるから，$G^{\varDelta}$ は $\varDelta$ 上2重可移である．□

問 8.1　G を7次の4重可移群とすると，$G=A_7$ または S_7 であることを示せ．

問 8.2　G を $\Omega=\{1,2,\cdots,n\}$ 上の4重可移群，P を G_{1234} の 2-シロー部分群とする．いま $|F(P)|=7$ であれば，$N_G(P)^{F(P)}=A_7$ であることを示せ．

問 8.3　G を $\Omega=\{1,2,\cdots,n\}$ 上の4重可移群，P を G_{1234} の 2-シロー部分群とし，$P\neq 1$ で $P-\{1\}$ の元はすべて $\Omega-F(P)$ 上に固定点をもたないとする．いま $|F(P)|=7$ であれば P は基本可換群になることを示せ．

問 8.4　G を $\Omega=\{1,2,\cdots,n\}$ 上の4重可移群，P を G_{1234} の 2-シロー部分群で，$1\lneqq P\trianglelefteq G_{1234}$ とする．いま $|F(P)|=7$ で，P は $\Omega-F(P)$ 上可移とすると，$n=23$ であることを示せ．

§9. 線形群

この節では次節で述べる重要な2重可移群である射影線形群を導くために，線形群について述べる．

体 K の元を成分とする n 次正則行列（行列式が0でない行列）全体の集合は，行列の積に関して群を作る．これを**一般線形群**（general linear group）といい，$GL(n,K)$ と書く．ここで K が有限体 $GF(q)$ のとき $GL(n,q)$ とも書く．

$$GL(n,K)\text{ の元}\begin{pmatrix}\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn}\end{pmatrix}\text{を略して }(\alpha_{ij})\text{ とも書く．}$$

一般線形群 $GL(n, K)$ の元 a で行列式 $\det a$ が 1 であるもの全体の集合は $GL(n, K)$ の部分群を作る．これを **特殊線形群** (special linear group) といい $SL(n, K)$ と書く．Kが有限体 $GF(q)$ のとき $SL(n, q)$ とも書く．

注 9.1 $GL(n, K) \trianglerighteq SL(n, K)$, $GL(n, K)/SL(n, K) \cong K^*$ である．

［証 明］ 任意の $a \in SL(n, K)$, 任意の $x \in GL(n, K)$ に対して，

$$\det(x^{-1}ax) = \det x^{-1} \cdot \det a \cdot \det x = (\det x)^{-1} \cdot 1 \cdot \det x = 1$$

であるから $x^{-1}ax \in SL(n, K)$ となり $GL(n, K) \trianglerighteq SL(n, K)$ である．

写像 $f : G(n, K) \to K^*, a \mapsto \det a$ は K^* の上への準同型写像で，$\ker f = SL(n, K)$ である．したがって定理 1;3.2 より $GL(n, K)/SL(n, K) \cong K^*$ である． □

以下 $GL(n, K)$ において $n \geqq 2$ とする．$GL(n, K)$ において，対角線成分がすべて 1，(i, j) 成分 $(i \neq j)$ が α で残りの成分はすべて 0 の行列を

$$a_{i,j}(\alpha) = \begin{pmatrix} 1 & & & & & \\ & 1 & & & 0 & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & \alpha & & \ddots & \\ 0 & & & & & 1 \end{pmatrix} \quad (\alpha \text{ は第 } i \text{ 行第 } j \text{ 列})$$

とおく．また (n, n) 成分が $\alpha\ (\neq 0)$，他の対角線成分が 1 で，残りの成分はすべて 0 の行列を

$$d(\alpha) = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ & & & 1 & \\ 0 & & & & \alpha \end{pmatrix}$$

とおく．

定 理 9.2

$$GL(n, K) = \langle a_{i,j}(\alpha), d(\alpha) \mid i, j = 1, 2, \cdots, n, \alpha \in K^* \rangle,$$

$$SL(n, K) = \langle a_{i,j}(\alpha) \mid i, j = 1, 2, \cdots, n, \alpha \in K^* \rangle$$

である．

［証 明］ 任意の $x \in GL(n, K)$ に対して

$a_{i,j}(\alpha) \cdot x$ は x の i 行に j 行の α 倍を加えた行列

$x \cdot a_{i,j}(\alpha)$ は x の j 列に i 列の α 倍を加えた行列

である．

したがって x に適当に i, j, α をえらんだ $a_{i,j}(\alpha)$ いくつかを左右からかけてゆくと $d(\alpha')$ となる．これより

$$GL(n, K) = \langle a_{i,j}(\alpha), d(\alpha) \mid i, j = 1, 2, \cdots, n, \alpha \in K^{\bullet} \rangle$$

である．

特に $x \in SL(n, K)$ のとき，$\det x = 1$, $\det a_{i,j}(\alpha) = 1$ であるから上で得られた $d(\alpha')$ は $\det d(\alpha') = 1$ となり，$d(\alpha')$ は単位行列になる．したがって

$$SL(n, K) = \langle a_{i,j}(\alpha) \mid i, j = 1, 2, \cdots, n, \alpha \in K^{\bullet} \rangle$$

である．□

系 9.3 $D(GL(n, K)), D(SL(n, K))$ をそれぞれ $GL(n, K)$, $SL(n, K)$ の交換子群とすると，$GL(2, 2), GL(2, 3)$ を除き

$$D(GL(n, K)) = D(SL(n, K)) = SL(n, K)$$

である．

［証 明］ 注 9.1 より $GL(n, K)/SL(n, K) \cong K^{\bullet}$ で $K^{\bullet}$ は可換群だから，定理 1;4.1 より

$$SL(n, K) \geqq D(GL(n, K)) \geqq D(SL(n, K))$$

である．定理 9.2 より $SL(n, K) = \langle a_{i,j}(\alpha) \rangle$ で $a_{i,j}(\alpha)^{-1} = a_{i,j}(-\alpha)$ である．これより $n \geqq 3$ のとき，$SL(n, K)$ の任意の生成元 $a_{i,j}(\alpha)$ に対して，$k \neq i, j$ をとると

$$a_{i,k}(\alpha)^{-1} a_{k,j}(1)^{-1} \cdot a_{i,k}(\alpha) \cdot a_{k,j}(1) = a_{i,j}(\alpha)$$

となり，$a_{i,j}(\alpha) \in D(SL(n, K))$ である．したがって

$$SL(n, K) = D(SL(n, K)) = D(GL(n, K))$$

が成り立つ．

$n = 2$ で $K \neq GF(2), GF(3)$ とする．このとき $\gamma^2 \neq 1$ である $\gamma \in K^{\bullet}$ が存在する．任意の $\alpha \in K^{\bullet}$ に対して，$\beta = \alpha(1 - \gamma^2)^{-1}$ とおくと $\begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix}$, $\begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix} \in SL(2, K)$ で

$$\begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix}^{-1} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta(1 - \gamma^2) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = a_{1,2}(\alpha),$$

$$\begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}^{-1} \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \beta(1 - \gamma^2) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} = a_{2,1}(\alpha)$$

より，$a_{1,2}(\alpha), a_{2,1}(\alpha) \in D(SL(2, K))$ となる．したがって

$$SL(2, K) = D(SL(2, K)) = D(GL(2, K))$$

が成り立つ．□

Vが体K上のn次元ベクトル空間のとき，$V(n,K)$と書く．ここでKが有限体$GF(q)$のとき，$V(n,q)$とも書く．

以下ベクトル空間の次元は2以上とする．

Vを体K上のベクトル空間とする．写像$\sigma:V\to V$が

$$(u+v)^\sigma=u^\sigma+v^\sigma,\quad (\lambda u)^\sigma=\lambda u^\sigma,\ {}^\forall u,\ v\in V,\ {}^\forall\lambda\in K$$

をみたすとき，σをVの**線形変換**という．特にσがV上の置換のとき，σを**正則な線形変換**という．

注 9.4 σをベクトル空間Vの正則な線形変換とすると，σの逆写像σ^{-1}が存在してVの正則な線形変換である．

［証明］ σはV上の置換であるから，置換としての逆元σ^{-1}が存在する．任意のu, $v\in V(n,K)$，任意の$\lambda\in K$に対して

$$(u+v)^{\sigma^{-1}}=(u^{\sigma^{-1}\sigma}+v^{\sigma^{-1}\sigma})^{\sigma^{-1}}=(u^{\sigma^{-1}}+v^{\sigma^{-1}})^{\sigma\sigma^{-1}}=u^{\sigma^{-1}}+v^{\sigma^{-1}},$$

$$(\lambda u)^{\sigma^{-1}}=(\lambda u^{\sigma^{-1}\sigma})^{\sigma^{-1}}=(\lambda u^{\sigma^{-1}})^{\sigma\sigma^{-1}}=\lambda u^{\sigma^{-1}}$$

であるから，σ^{-1}も正則な線形変換である．□

したがって，ベクトル空間Vの正則な線形変換全体の集合は，明らかにV上の置換群を作り，これを$GL(V)$と書く．

注 9.5 $\{v_1,v_2,\cdots,v_n\}$をベクトル空間$V=V(n,K)$の基とする．このとき$\sigma\in GL(V)$に対して$\{v_1^\sigma,v_2^\sigma,\cdots,v_n^\sigma\}$は$V$の基である．

逆に$\{u_1,u_2,\cdots,u_n\}$をVの任意の基とするとき，$v_i^\sigma=u_i$ $(i=1,2,\cdots,n)$となる$\sigma\in GL(V)$が一意的に存在する．

［証明］ $\sigma\in GL(V)$をとる．任意の$v=\sum_{i=1}^n\lambda_iv_i\in V$ $(\lambda_i\in K)$に対して$v^\sigma=(\sum_{i=1}^n\lambda_i\cdot v_i)^\sigma=\sum_{i=1}^n\lambda_iv_i^\sigma$である．ここで$V=\{v^\sigma|v\in V\}$であるから，$V$の任意の元$v^\sigma$は$v_1^\sigma$, $v_2^\sigma,\cdots,v_n^\sigma$の1次結合で書け，したがって$\{v_1^\sigma,v_2^\sigma,\cdots,v_n^\sigma\}$は$V$の基である．

逆に写像$\sigma:V\to V$を$v=\sum_{i=1}^n\lambda_iv_i$に対して$v^\sigma=\sum_{i=1}^n\lambda_iu_i$により定義する．このとき$v_i^\sigma=u_i$ $(i=1,2,\cdots,n)$で明らかに$\sigma\in GL(V)$である．いま$\tau\in GL(V)$で$v_i^\tau=u_i$ $(i=1,2,\cdots,n)$とすると，$\sigma\tau^{-1}\in GL(V)$で$v_i^{\sigma\tau^{-1}}=v_i$ $(i=1,2,\cdots,n)$となり$\sigma\tau^{-1}=1$, $\sigma=\tau$である．□

$\{v_1,v_2,\cdots,v_n\}$をベクトル空間$V=V(n,K)$の基とする．このとき$v\in V$は$v=\sum_{i=1}^n\lambda_iv_i$と一意的に書けるから，$v=(\lambda_1,\lambda_2,\cdots,\lambda_n)$と書き，$(\lambda_1,\lambda_2,\cdots,$

λ_n）を基 $\{v_1, v_2, \cdots, v_n\}$ に関する v の座標という．また $u=(\mu_1, \mu_2, \cdots, \mu_n)$ とすると $u+v=(\lambda_1+\mu_1, \lambda_2+\mu_2, \cdots, \lambda_n+\mu_n)$ である．

ベクトル空間 $V=V(n, K)$ の基 $\{v_1, v_2, \cdots, v_n\}$ を定めて，$GL(n, K)$ の元 $a=(\alpha_{ij})$ による V から V への写像をつぎのように定義する．

$v=(\lambda_1, \lambda_2, \cdots, \lambda_n)\in V$ に対して，a による v の像 v^a を行列 $(\lambda_1\ \lambda_2\ \cdots\ \lambda_n)$ と行列 (α_{ij}) の行列としての積

$$(\lambda_1\ \lambda_2\ \cdots\ \lambda_n)(\alpha_{ij})=(\sum_{i=1}^{n}\lambda_i\alpha_{i1}\ \ \sum_{i=1}^{n}\lambda_i\alpha_{i2}\ \ \cdots\ \ \sum_{i=1}^{n}\lambda_i\alpha_{in})$$

により，$v^a=(\sum_{i=1}^{n}\lambda_i\alpha_{i1}, \sum_{i=1}^{n}\lambda_i\alpha_{i2}, \cdots, \sum_{i=1}^{n}\lambda_i\alpha_{in})$ とする．

定理 9.6 ベクトル空間 $V=V(n,K)$ の基 $\{v_1, v_2, \cdots, v_n\}$ を定める．このとき $a\in GL(n,K)$ による写像は V 上の正則な線形変換で，これにより $GL(n,K)$ は V 上の置換群となり $GL(V)$ と V 上の置換群として同値である．

ここで $\sigma\in GL(V)$ により $v_i{}^\sigma=\sum_{j=1}^{n}\alpha_{ij}v_j$ $(j=1,2,\cdots,n)$ すなわち

$$\begin{pmatrix} v_1{}^\sigma \\ v_2{}^\sigma \\ \vdots \\ v_n{}^\sigma \end{pmatrix}=(\alpha_{ij})\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

とすると，σ と V 上の置換として一致する $GL(n,K)$ の元は (α_{ij}) である．

［証 明］ 任意の $u,v\in V$ に対して，行列の演算に関する性質より

$$(u+v)^a=u^a+v^a,\ (\lambda u)^a=\lambda u^a,\ \lambda\in K$$

が成り立つ．したがって a による写像は V の線形変換である．

任意の $a,b\in GL(n,K)$，任意の $v\in V$ に対して，行列の積についての結合法則より，$v^{(ab)}=(v^a)^b$ である．したがって a と b の積 ab による写像は a と b の写像としての積に一致する．さらに a の逆元 a^{-1} は V 上の写像として a の逆写像になるから，a は V 上の置換である．

以上より $GL(n, K)$ は V に作用するが，$GL(n, K)$ の異なる2元は明らかに V 上の置換としても異なるから，$GL(n,K)$ は V 上の置換群となり，$GL(V)$ の部分群と同値である．

任意の $\sigma\in GL(V)$ に対して

$$\begin{pmatrix} v_1{}^\sigma \\ v_2{}^\sigma \\ \vdots \\ v_n{}^\sigma \end{pmatrix}=(\alpha_{ij})\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

とする．このとき任意の $v=\sum_{i=1}^{n}\lambda_i v_i \in V$ に対して，

$$v^\sigma=\sum_{i=1}^{n}\lambda_i v_i{}^\sigma=\sum_{i=1}^{n}\lambda_i\Big(\sum_{j=1}^{n}\alpha_{ij}v_j\Big)=\sum_{j=1}^{n}\Big(\sum_{i=1}^{n}\lambda_i\,\alpha_{ij}\Big)v_j$$

となる．したがって $a=(\alpha_{ij})$ とおくと $v^\sigma=v^a$ となり，σ と a は V 上の置換として一致し，a の逆元は σ^{-1} よりえられるから $a\in GL(n,K)$ となる．

以上より $GL(n,K)$ は V 上の置換群として $GL(V)$ と同値である．□

$v=(\lambda_1,\lambda_2,\cdots,\lambda_n)$, $a=(\alpha_{ij})$ のとき $v^a=(\lambda_1,\ \lambda_2,\cdots,\lambda_n)^{(\alpha_{ij})}$ と書く．また $V(n,K)$ の基のとり方を変えると $GL(n,K)$ の V 上の作用は異なる．

V の基を定めたとき，V 上の置換として一致する $GL(n,K)$ と $GL(V)$ の元を対応する元ということにする．

補 題 9.7 $\sigma\in GL(V)$ に対して $V=V(n,K)$ の2つの基 $\{v_1,v_2,\cdots,v_n\}$ および $\{u_1,u_2,\cdots,u_n\}$ により対応する $GL(n,K)$ の元をそれぞれ $(\alpha_{ij}),(\beta_{ij})$ とする．

いま $\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=(\gamma_{ij})\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}$ とすると

$$(\gamma_{ij})(\alpha_{ij})=(\beta_{ij})(\gamma_{ij})$$

である．

したがって σ に対応する $GL(n,K)$ の元の行列式は，V の基のとり方にかかわらず一定となり，これを σ の行列式といい $\det\sigma$ と書く．

［証 明］ 仮定より定理 9.6 を用いて

$$\begin{pmatrix}v_1{}^\sigma\\v_2{}^\sigma\\\vdots\\v_n{}^\sigma\end{pmatrix}=(\alpha_{ij})\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix},\qquad\begin{pmatrix}u_1{}^\sigma\\u_2{}^\sigma\\\vdots\\u_n{}^\sigma\end{pmatrix}=(\beta_{ij})\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}$$

である．さらに $\{v_1,\ v_2,\cdots,v_n\}$，$\{u_1,\ u_2,\cdots,u_n\}$ は共に V の基であるから，注 9.5 より $\tau\in GL(V)$ が存在して $v_i{}^\tau=u_i\ (i=1,2,\cdots,n)$ である．

したがって $\{v_1,v_2,\cdots,v_n\}$ により τ に対応する行列は

$$\begin{pmatrix}v_1{}^\tau\\v_2{}^\tau\\\vdots\\v_n{}^\tau\end{pmatrix}=\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=(\gamma_{ij})\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}$$

より (γ_{ij}) となり，$(\gamma_{ij})\in GL(n,K)$ である．このとき

$$\begin{pmatrix} u_1{}^\sigma \\ u_2{}^\sigma \\ \vdots \\ u_n{}^\sigma \end{pmatrix} = (\gamma_{ij}) \begin{pmatrix} v_1{}^\sigma \\ v_2{}^\sigma \\ \vdots \\ v_n{}^\sigma \end{pmatrix} = (\gamma_{ij})(\alpha_{ij}) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

であり，

$$\begin{pmatrix} u_1{}^\sigma \\ u_2{}^\sigma \\ \vdots \\ u_n{}^\sigma \end{pmatrix} = (\beta_{ij}) \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = (\beta_{ij})(\gamma_{ij}) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

でもある．したがってこの2つの式より $(\gamma_{ij})(\alpha_{ij}) = (\beta_{ij})(\gamma_{ij})$ である．

ここで $\det(\gamma_{ij})\cdot\det(\alpha_{ij}) = \det(\beta_{ij})\cdot\det(\gamma_{ij})$，$\det(\gamma_{ij}) \neq 0$ より，$\det(\alpha_{ij}) = \det(\beta_{ij})$ である．□

$SL(V) = \{\sigma\in GL(V) \mid \det\sigma = 1\}$ は明らかに $GL(V)$ の部分群である．ここで $V(n, K)$ の基を定めると，定理9.6よりV上の置換群として $SL(n, K)$ は $SL(V)$ と同値である．

σを $V = V(n, K)$ からVへの写像とする．いまσによって定まるKの自己同型θが存在して

$$(u+v)^\sigma = u^\sigma + v^\sigma$$
$$(\lambda u)^\sigma = \lambda^\theta u^\sigma \qquad (\forall u, v\in V, \forall\lambda\in K)$$

が成り立つとき，σ を V の **半線形変換**，θをσに属する体Kの自己同型という．σを σ_θ と書くときもある．

特にσがV上の置換のとき，σを正則な半線形変換という．

半線形変換 σ_θ で $\theta = 1$ のときが線形変換である．また有限体 $GF(p^r)$（pは素数）において Aut $GF(p^r)$ は定理 1;5.3 に述べたように位数rの巡回群$\langle\theta\rangle$，$\theta^i : \xi\mapsto\xi^{p^i}, \forall\xi\in GF(p^r)$ である．したがって $V(n, p^r)$ の半線形変換は，任意の $u\in V(n, p^r)$，任意の $\lambda\in GF(p^r)$ に対して，$(\lambda u)^\sigma = \lambda^{p^i} u^\sigma$ である．

注 9.8 $\sigma_{\theta_1}, \tau_{\theta_2}$ を $V = V(n, K)$ の半線形変換とする．このときσとτの写像としての積 $\sigma\tau$ も半線形変換で，$\theta_1\theta_2$ が $\sigma\tau$ に属する Aut K の元である．したがって正則な半線形変換全体は，V上の置換群を作る．

［証明］ 任意の $u, v\in V$，任意の $\lambda\in K$ に対して

$$(u+v)^{\sigma\tau} = ((u+v)^\sigma)^\tau = (u^\sigma + v^\sigma)^\tau = u^{\sigma\tau} + v^{\sigma\tau},$$
$$(\lambda u)^{\sigma\tau} = ((\lambda u)^\sigma)^\tau = (\lambda^{\theta_1} u^\sigma)^\tau = \lambda^{\theta_1\theta_2} u^{\sigma\tau}$$

が成り立ち，$\theta_1\theta_2 \in \mathrm{Aut}\, K$ であるから，$\sigma\tau$ は半線形変換で，$\theta_1\theta_2$ が $\sigma\tau$ に属する $\mathrm{Aut}\, K$ の元である．

特に σ_θ が正則のとき，置換としての逆元は，注 9.4 の証明と同様にして，自己同型 θ^{-1} をもつ正則な半線形変換であり，正則な半線形変換全体の集合は V 上の置換群を作ることはみやすい．□

$V=V(n,K)$ の正則な半線形変換全体の作る群を**一般半線形群**といい，$\Gamma L(V)$ または $\Gamma L(n,K)$ と書く．K が有限体 $GF(q)$ のとき $\Gamma L(n,q)$ とも書く．

補題 9.9 $\{v_1, v_2, \cdots, v_n\}$ をベクトル空間 $V=V(n,K)$ の基とし，任意の $v\in V$ の $\{v_1, v_2, \cdots, v_n\}$ による座標を $v=(\lambda_1, \lambda_2, \cdots, \lambda_n)$ とする．

このとき $\sigma=\sigma_\theta \in \Gamma L(V)$ に対して，$(\alpha_{ij})\in GL(n,K)$ が定まり，任意の $v=(\lambda_1, \lambda_2, \cdots, \lambda_n)\in V$ に対して，$v^\sigma=(\lambda_1{}^\theta, \lambda_2{}^\theta, \cdots, \lambda_n{}^\theta)^{(\alpha_{ij})}$ である．

逆に $v^\sigma=(\lambda_1{}^\theta, \lambda_2{}^\theta, \cdots, \lambda_n{}^\theta)^{(\alpha_{ij})}$, $\theta\in \mathrm{Aut}\, K, (\alpha_{ij})\in GL(n,K)$ で定義される V から V への写像 σ は，θ を自己同型としてもつ $\Gamma L(V)$ の元である．

［証 明］ 基を作るベクトル $v_1, v_2, \cdots, v_n$ に対して $\sigma=\sigma_\theta\in \Gamma L(V)$ が

$$\begin{pmatrix} v_1{}^\sigma \\ v_2{}^\sigma \\ \vdots \\ v_n{}^\sigma \end{pmatrix} = (\alpha_{ij}) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

とする．このとき任意の $v=\sum_{i=1}^n \lambda_i v_i \in V$ に対して

$$v^\sigma=\sum_{i=1}^n (\lambda_i v_i)^\sigma = \sum_{i=1}^n \lambda_i{}^\theta\, v_i{}^\sigma = \sum_{i=1}^n \lambda_i{}^\theta \Big(\sum_{j=1}^n \alpha_{ij} v_j\Big) = \sum_{j=1}^n \Big(\sum_{i=1}^n \lambda_i{}^\theta \alpha_{ij}\Big) v_j$$

となり，$GL(n,K)$ の元による写像と同様な表し方を用いて，$v^\sigma=(\lambda_1{}^\theta, \lambda_2{}^\theta, \cdots, \lambda_n{}^\theta)^{(\alpha_{ij})}$ となる．さらに σ の逆元 σ^{-1} に対して同様に $v^{\sigma^{-1}}=(\lambda_1{}^{\theta^{-1}}, \lambda_2{}^{\theta^{-1}}, \cdots, \lambda_n{}^{\theta^{-1}})^{(\beta_{ij})}$ となり

$$v=(v^{\sigma^{-1}})^\sigma=(\lambda_1{}^{\theta^{-1}\theta}, \lambda_2{}^{\theta^{-1}\theta}, \cdots, \lambda_n{}^{\theta^{-1}\theta})^{(\beta_{ij}{}^\theta)(\alpha_{ij})}=(\lambda_1, \lambda_2, \cdots, \lambda_n)^{(\beta_{ij}{}^\theta)(\alpha_{ij})}$$

より，$(\beta_{ij}{}^\theta)(\alpha_{ij})=1, (\alpha_{ij})\in GL(n,K)$ である．

逆に任意の $v=(\lambda_1, \lambda_2, \cdots, \lambda_n)\in V$ に対して $v^\sigma=(\lambda_1{}^\theta, \lambda_2{}^\theta, \cdots, \lambda_n{}^\theta)^{(\alpha_{ij})}$, $\theta\in \mathrm{Aut}\, K$, $(\alpha_{ij})\in GL(n, K)$ により定義される V から V への写像とすると，σ は明らかに θ を自己同型としてもつ $\Gamma L(V)$ の元である．□

定 理 9.10 $V=V(n,K)$ をベクトル空間，$\{v_1, v_2, \cdots, v_n\}$ を V の基とする．$\theta\in \mathrm{Aut}\, K$ に対して，V から V への写像 Θ を任意の $v=\sum_{i=1}^n \lambda_i v_i\in V$ に対して，$v^\Theta=\sum_{i=1}^n \lambda_i{}^\theta v_i$ と定義するとき，$\Theta\in \Gamma L(V)$ となり $\Gamma L(V)=\{\Theta\sigma \mid \theta\in \mathrm{Aut}\, K,$

$\sigma \in GL(V)\}$ である．

これより $\Gamma L(V) \trianglerighteq GL(V)$，$\Gamma L(V)/GL(V) \cong \mathrm{Aut}\, K$ となる．

［証 明］ $v = (\lambda_1, \lambda_2, \cdots, \lambda_n) \in V$ に対して $v^\Theta = (\lambda_1{}^\theta, \lambda_2{}^\theta, \cdots, \lambda_n{}^\theta)^1$，1は単位行列，であるから補題 9.9 より $\Theta \in \Gamma L(V)$ である．

任意の $\sigma = \sigma_\theta \in \Gamma L(V)$ に対して，補題 9.9 より

$$v^\sigma = (\lambda_1{}^\theta, \lambda_2{}^\theta, \cdots, \lambda_n{}^\theta)^{(\alpha_{ij})} = (\lambda_1, \lambda_2, \cdots, \lambda_n)^{\Theta\cdot(\alpha_{ij})}, \qquad (\alpha_{ij}) \in GL(n, K)$$

で，定理 9.6 より $(GL(n, K), V) \cong (GL(V), V)$ であるから

$$\Gamma L(V) = \{\Theta\sigma \mid \theta \in \mathrm{Aut}\ K, \sigma \in GL(V)\}$$

となる．

写像 $f: \Gamma L(V) \to \mathrm{Aut}\, K$ を $\sigma_\theta \mapsto \theta$ により定義する．任意の $\sigma_{\theta_1}, \tau_{\theta_2} \in \Gamma L(V)$ に対して注 9.8 より $(\sigma_{\theta_1}\tau_{\theta_2})^f = \theta_1\theta_2$ であるから，f は準同型である．さらに f は明らかに全射で，$\ker f = GL(V)$ であるから，

$$\Gamma L(V) \trianglerighteq GL(V), \qquad \Gamma L(V)/GL(V) \cong \mathrm{Aut}\, K$$

が成り立つ．□

注 9.11 $\sigma \in GL(V)$ に対応する行列を (α_{ij}) とすると，$\sigma^\theta = \Theta^{-1}\sigma\Theta$ $(\theta \in \mathrm{Aut}\, K)$ に対応する行列は $(\alpha_{ij}{}^\theta)$ である．

［証 明］ $v = (\lambda_1, \lambda_2, \cdots, \lambda_n) \in V$ に対して

$$v^{\Theta^{-1}\sigma\Theta} = (\lambda_1, \lambda_2, \cdots, \lambda_n)^{\Theta^{-1}\sigma\Theta} = (\lambda_1{}^{\theta^{-1}}, \lambda_2{}^{\theta^{-1}}, \cdots, \lambda_n{}^{\theta^{-1}})^{\sigma\Theta}$$
$$= ((\lambda_1{}^{\theta^{-1}}, \lambda_2{}^{\theta^{-1}}, \cdots, \lambda_n{}^{\theta^{-1}})^{(\alpha_{ij})})\theta = (\lambda_1, \lambda_2, \cdots, \lambda_n)^{(\alpha_{ij}{}^\theta)}$$

であるから σ^θ に対応する行列は $(\alpha_{ij}{}^\theta)$ である．□

系 9.12 p を素数とするとき，$\Gamma L(n, p) = GL(n, p)$ である．

［証 明］ $\mathrm{Aut}\, GF(p) = 1$ だから定理 9.10 より成り立つ．□

定 理 9.13 G を位数 p^n（p は素数）の基本可換群とすると，$(\mathrm{Aut}\, G, G) \cong (GL(n, p),\ V(n, p))$ である．

［証 明］ 定理 1;2.4 より G は n 個の位数 p の巡回群の直積 $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$ である．またベクトル空間 $V(n, p)$ の基を $\{v_1, v_2, \cdots, v_n\}$ とする．G の元（$\neq 1$）はすべて位数が p で，$V(n, p)$ は標数 p の素体上のベクトルよりなるから，写像 $\varphi: G \to V$ を

$$a_1{}^{r_1} a_2{}^{r_2} \cdots a_n{}^{r_n} \mapsto r_1 v_1 + r_2 v_2 + \cdots + r_n v_n$$

により定義できる．このとき写像 φ は明らかに全単射である．

つぎに $\sigma\in\mathrm{Aut}\,G$ に対して $a_i^{\sigma}=\prod_{j=1}^{n}a_j^{r_{ij}}\,(i=1,2,\cdots,n)$ とすると，任意の $x=\prod_{i=1}^{n}a_i^{r_i}\in G$ に対して

$$x^{\sigma}=\prod_{i=1}^{n}(a_i^{r_i})^{\sigma}=\prod_{i=1}^{n}(\prod_{j=1}^{n}a_j^{r_{ij}})^{r_i}=\prod_{j=1}^{n}(a_j^{\Sigma r_i r_{ij}})$$

となり，$\mathrm{Aut}\,G$ の元は生成元 $a_1, a_2,\cdots,a_n$ の像により一意的に決まるから，σ に対して一意的に行列 (r_{ij}) が決まる．いま σ^{-1} により $a_i^{\sigma^{-1}}=\prod_{j=1}^{n}a_j^{s_{ij}}\ (i=1,2,\cdots,n)$ とすると $a_i=a_i^{\sigma^{-1}\sigma}=(\prod_{j=1}^{n}a_j^{s_{ij}})^{\sigma}=\prod_{k=1}^{n}(a_k^{\Sigma s_{ij}r_{jk}})$ となり，$(s_{ij})\,(r_{ij})=1$ より $(r_{ij})\in GL(n,p)$ である．したがって写像 $f:\mathrm{Aut}\,G\to GL(n,p)$ を，上の $\sigma\mapsto(r_{ij})$ により決める．このとき写像 f も明らかに全単射である．

任意の $x=\prod_{i=1}^{n}a_i^{r_i}\in G$，任意の $\sigma\in\mathrm{Aut}\,G$ に対して

$$(x^{\sigma})^{\varphi}=(\prod_{j=1}^{n}a_j^{\Sigma r_i r_{ij}})^{\varphi}=\sum_{j=1}^{n}(\sum_{i=1}^{n}r_ir_{ij})v_j$$

$$(x^{\varphi})^{\sigma^f}=(\sum_{i=1}^{n}r_iv_i)^{\sigma^f}=\sum_{j=1}^{n}(\sum_{i=1}^{n}r_ir_{ij})v_j$$

より $(x^{\sigma})^{\varphi}=(x^{\varphi})^{\sigma^f}$ が成り立ち，$(\mathrm{Aut}G, G)\cong(GL(n,p), V(n,p))$ である．□

定理 9.14　(1)　$|GL(n,q)|=(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

(2)　$|SL(n,q)|=|GL(n,q)|/(q-1)$.

(3)　p を素数とすると，$|\Gamma L(n,p^r)|=r\cdot|GL(n,p^r)|$.

［**証明**］(1)　$V=V(n,q)$ の順序を考えた基，すなわち基 $\{v_1,v_2,\cdots,v_n\}$ に対してベクトル $v_1, v_2,\cdots,v_n$ の並び方を変えた基は $\{v_1, v_2,\cdots,v_n\}$ と異なるとした V の基の個数は，注 9.5 より $GL(n,q)$ の位数に等しい．

順序を考えた V の基 $\{v_1,v_2,\cdots,v_n\}$ の個数は，v_1 として $V-\{0\}$ の任意のベクトルをとりうるから，q^n-1 通りのとり方がある．v_1 を決めたとき，v_2 として $V-\langle v_1\rangle$ の任意のベクトルをとりうるから，q^n-q 通りのとり方がある．v_1,v_2 を決めたとき，v_3 として $V-\langle v_1,v_2\rangle$ の任意のベクトルをとりうるから，q^n-q^2 通りのとり方がある．以下同様に続けて $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$ 個の順序を考えた基が存在し，これは $|GL(n,q)|$ に等しい．

(2)　注 9.1 より $|SL(n,q)|=|GL(n,q)|/(q-1)$ である．

(3)　定理 1;5.3 より $|\mathrm{Aut}\,GF(p^r)|=r$ であるから，定理 9.10 より $|\Gamma L(n,p^r)|=r\cdot|GL(n,p^r)|$ である．□

問 9.1　$GL(n,q)$ は，位数 q^n-1 の巡回群 H をもち，H は $V(n,p)-\{0\}$ 上可移であることを示せ．

問 9.2　$V(n,q)$ の m 次元部分ベクトル空間の全体の集合の上で，$SL(V)$ は可移で

あることを示せ.

問 9.3　$V(n,q)$ の $n-1$ 次元部分ベクトル空間を**超平面**という. またVの超平面Uに対して $GL(V)$ の元τで, $u^\tau=u$ $(u\in U)$, $v^\tau-v\in U$ $(v\in V)$ をみたすものを, VのUに関する**移換** (transvection) という.

(1)　$GF(q)$ を $GF(q)$ 上の1次元ベクトル空間とみなし, f をVから$GF(q)$ 上への線形写像 (**線形関数**という) とするとき, $\ker f=\{v\in V\mid v^f=0\}$ はVの超平面であることを示せ. 逆にVの超平面Uに対して, $\ker f=U$ となるVの線形関数が存在することを示せ.

(2)　UをVの超平面, τをUに関するVの移換, fを $\ker f=U$ となるVの線形関数とする. このとき $v_0(\neq 0)\in V$ が存在して, $v^\tau=v-v^fv_0$ $(v\in V)$ となることを示せ.

(3)　逆にfをVの線形関数, $v_0(\neq 0)\in V$ を $v_0{}^f=0$ とする. いまVからVへの写像τが, $v^\tau=v-v^fv_0$ $(v\in V)$ をみたすとき, τは超平面 $\ker f$に関する移換であることを示せ.

(4)　移換の全体は $SL(V)$ を生成することを示せ.

§10. 射影線形群

この節においてもベクトル空間の次元は2以上とする.

またベクトル空間 $V=V(n,K)$ の基を定めることより, V上の置換群として $(GL(n,K),V)\cong(GL(V),V)$ であるから, Vの基をあらかじめ定めることにより, $GL(n,K)$ をV上の置換群 $GL(V)$ として扱う.

補題 10.1　$G=\Gamma L(V)$ は $V=V(n,K)$ 上の置換群で, 2つの軌道 $\{0\}$ と$V^\sharp=V-\{0\}$ をもつ.

$V^\sharp$ 上 $[v]=\{\alpha v\mid \alpha\in K^\sharp(K^\sharp=K-\{0\})\}$ $(0\notin[v])$ とおくと, $[v]$ はGの非原始ブロックである. したがって $K=GF(2)$ を除き, Gは$V^\sharp$上の置換群として, $\{[v]\mid v\in V^\sharp\}$ を非原始系とする非原始置換群である.

[証 明]　GはVに作用するが, Vの恒等写像になるのはGの単位元のみであるから, GはV上の置換群である. このときV上のG-軌道は明らかに $\{0\}$ と$V^\sharp$である.

任意の $\sigma=\sigma_\theta\in G$ に対して　$[v]^\sigma=\{\alpha v\mid\alpha\in K^\sharp\}^\sigma=\{\alpha^\theta v^\sigma\mid\alpha\in K^\sharp\}=[v^\sigma]$　である. したがって, $u\in[v]\cap[v^\sigma]$ であれば $u=\alpha v=\alpha' v^\sigma$ $(\alpha,\alpha'\in K^\sharp)$ より $[v]=[\alpha^{-1}\alpha' v^\sigma]=[v^\sigma]$ となり, $[v]$ はGの非原始ブロックである. $K\neq GF(2)$ であれば, $1<|[v]|<$

$|V^\sharp|$ であるから $[v]$ はGの自明でない非原始ブロックとなり，Gは$V^\sharp$上 $\{[v]|v\in V^\sharp\}$ を非原始系とする非原始置換群である．□

$V(n,2)$ に対しては $[v]=\{v\}$ であるから $\{[v]|v\in V^\sharp\}$ は $V(n,2)^\sharp$ に一致する．

補題 10.2　補題10.1の非原始系 $\{[v]|v\in V^\sharp\}$ 上 $\Gamma L(V)$ の作用の核は $Z(V)=\{\alpha\cdot 1_V|\alpha\in K^\sharp, 1_V$ は V の恒等写像$\}$ である．

[証明]　$Z(V)$ の元は明らかに $\{[v]|v\in V^\sharp\}$ 上の恒等写像である．

逆に $\sigma\in\Gamma L(V)$ がすべての $v\in V^\sharp$ に対して $[v]^\sigma=[v]$ とする．$[v]^\sigma=[v^\sigma]$ より $v^\sigma=\alpha_v\cdot v$ となる $\alpha_v\in K^\sharp$ が存在する．したがって任意の $v_1, v_2\in V$ に対して $v_1{}^\sigma=\alpha_1 v_1$, $v_2{}^\sigma=\alpha_2 v_2$, α_1, $\alpha_2\in K^\sharp$ となる．

いま v_1 と v_2 が1次独立とする．このとき仮定より

$$(v_1+v_2)^\sigma=\alpha'(v_1+v_2)=\alpha' v_1+\alpha' v_2,\ \ \alpha'\in K^\sharp$$

である．一方 σ は半線形変換だから

$$(v_1+v_2)^\sigma=v_1{}^\sigma+v_2{}^\sigma=\alpha_1 v_1+\alpha_2 v_2$$

である．したがって

$$\alpha' v_1+\alpha' v_2=\alpha_1 v_1+\alpha_2 v_2$$

となり，v_1 と v_2 は1次独立だから $\alpha'=\alpha_1=\alpha_2$ となる．

v_1 と v_2 が1次独立でないとする．V の次元は2以上だから，v_1, v_2 に1次独立な $u\in V$ が存在する．このとき $u^\sigma=\beta u$ とすると上と同様にして，$\alpha_1=\beta$, $\alpha_2=\beta$ となり $\alpha_1=\alpha_2$ である．

以上より任意の $v\in V$ に対して $v^\sigma=\alpha\cdot v=v^{\alpha\cdot 1_V}$ となり，$\sigma=\alpha\cdot 1_V\in Z(V)$ である．すなわち $\Gamma L(V)$ の核は $Z(V)$ である．□

注 10.3　ベクトル空間 $V=V(n,K)$ において

$$Z(V)=Z(GL(V));\ \ GL(V) \text{ の中心}$$

である．さらに $Z(n,K)=\{\alpha\cdot 1|\alpha\in K^\sharp$, 1は単位行列$\}$ とおくと，$Z(n,K)$ は $GL(n,K)$ の部分群でVの基のとり方に関係なくVへの作用が定まり

$$(Z(V),V)\cong(Z(n,K),V)$$

である．

[証明]　$Z(V)$ は $GL(V)$ の部分群で，$Z(GL(V))$ に含まれることは明らかである．

逆に任意の $\sigma\in Z(GL(V))$をとる．任意の $v_1\in V^\sharp$ に対して，v_1 を含むVの基 $\{v_1, v_2,$

$\cdots, v_n\}$ をとると，$\{v_1, v_2, \cdots, v_j + v_1, \cdots, v_n\}$ $(j \neq 1)$ も V の基である．いま $v_1^{\sigma} = \sum_{i=1}^{n} \lambda_i v_i$ とすると，注 9.5 より $GL(V)$ に $v_i^{\tau} = v_i$ $(i \neq j)$, $v_j^{\tau} = v_j + v_1$ である元 τ が存在する．ここで $v_1^{\sigma\tau} = v_1^{\tau\sigma}$ であるから

$$v_1^{\sigma\tau} = (\sum_{i=1}^{n} \lambda_i v_i)^{\tau} = \sum_{i=1}^{n} \lambda_i v_i + \lambda_j v_1 = v_1^{\sigma} + \lambda_j v_1,$$
$$v_1^{\tau\sigma} = v_1^{\sigma}$$

である．したがって $v_1^{\sigma} + \lambda_j v_1 = v_1^{\sigma}$, $\lambda_j = 0$ となる．いま j として $2, 3, \cdots, n$ ととることにより，$v_1^{\sigma} = \lambda_1 v_1$, $[v_1]^{\sigma} = [v_1]$ となる．ここで v_1 は $V^{\#}$ の任意のベクトルであるから，$\sigma \in Z(V)$ となり $Z(V) = Z(GL(V))$ である．

$Z(n, K)$ は $GL(n, K)$ の部分群で，任意の $v \in V$ に対して $\alpha \cdot 1 \in Z(n, K)$ は V の基のとり方に関係なく $v^{\alpha \cdot 1} = \alpha v$ である．これより $\alpha \cdot 1_V \in Z(V)$ と $\alpha \cdot 1 \in Z(n, K)$ は V 上の置換として同じであるから，

$$(Z(V), V) \cong (Z(n, K), V)$$

である．□

以下 $v \in V^{\#}$ に対して $[v] = \{\alpha v | \alpha \in K^{\#}\}$ とする．補題 10.2 で示したことより $\Gamma L(V)/Z(V)$ は $\{[v] | v \in V^{\#}\}$ 上の置換群である．$\Gamma L(V)$ の元 σ を含む $\Gamma L(V)/Z(V)$ の剰余類を $[\sigma]$ と書く．このとき $(\alpha \cdot 1_V) \cdot \sigma = \alpha\sigma$ $(\alpha \in K^{\#})$ と書くと $[\sigma] = [\alpha\sigma]$, $[v]^{[\sigma]} = [v^{\sigma}]$ である．

$[v]$ に零ベクトルを加えて $[v] = \{\alpha v | \alpha \in K\}$ と定義する場合もあるが，本書では用いない．ただこれから述べることについて，いずれを用いても違いは生じない．

ベクトル空間 $V = V(n, K)$ に対して $\{[v] | v \in V^{\#}\}$ を $[v]$ を点とする体 K 上の $n-1$ 次元**射影空間** (projective space) といい，$PG(V)$ または $PG(n-1, K)$ と書く．また $K = GF(q)$ のとき $PG(n-1, q)$ とも書く．V の r 次元部分空間 U に対して $[U] = \{[u] | u \in V^{\#}\}$ を $PG(V)$ の $r-1$ 次元**部分空間**という．特に $PG(V)$ の 1 次元部分空間を**直線**，2 次元部分空間を**平面**という．また $PG(1, K)$ を体 K 上の**射影直線** (projective line), $PG(2, K)$ を体 K 上の**射影平面** (projective plane) という．

$\Gamma L(V)/Z(V)$ を $P\Gamma L(V), P\Gamma L(n, K)$ または $P\Gamma L(n, q)$ と書き**射影一般半線形群**という．$P\Gamma L(n, K)$ は補題 10.2 より $PG(n-1, K)$ 上の置換

群である．いま $PGL(V)=GL(V)/Z(V)$, $PSL(V)=SL(V)/(Z(V)\cap SL(V))$, $PGL(n,K)=GL(n,K)/Z(n,K)$, $PSL(n,K)=SL(n,K)/(Z(n,K)\cap SL(n,K))$ とおく．

定理9.6 より $V(n,K)$ 上の置換群として，$(GL(V),V)\cong(GL(n,K),V)$, $(SL(V),V)\cong(SL(n,K),V)$ であり，注 10.3 より $(Z(V),V)\cong(Z(n,K),V)$ であるから $PG(n-1,K)$ 上の置換群として

$$(PGL(V),PG(n-1,K))\cong(PGL(n,K),PG(n-1,K))$$
$$(PSL(V),PG(n-1,K))\cong(PSL(n,K),PG(n-1,K))$$

である．したがって $V(n,K)$ の基をあらかじめ定めることにより，$PGL(n,K)$, $PSL(n,K)$ をそれぞれ $PG(n-1,K)$ 上の置換群 $PGL(V)$, $PSL(V)$ として扱う．さらに定理 1;3.3 より $PSL(n,K)\cong SL(n,K)\cdot Z(n,K)/Z(n,K)$ であるから，この同型対応により $PSL(n,K)$ を $PGL(n,K)$ の部分群とみなすことができる．また $a=(\alpha_{ij})\in GL(n,K)$ に対して a を含む $PGL(n,K)$ の剰余類を $[a]=[\alpha_{ij}]$ と書く．

$PGL(n,K)$ を**射影一般線形群** (projective general linear group) といい，$PSL(n,K)$ を**射影特殊線形群** (projective special linear group) という．$K=GF(q)$ のときそれぞれ $PGL(n,q)$, $PSL(n,q)$ とも書く．

定理 10.4 （1） $|PG(n,q)|=(q^{n+1}-1)/(q-1)=q^n+q^{n-1}+\cdots+q+1$

（2） $|P\Gamma L(n,q)|=|\Gamma L(n,q)|/(q-1)$

（3） $|PGL(n,q)|=|GL(n,q)|/(q-1)$

（4） $|PSL(n,q)|=|SL(n,q)|/(n,q-1)$. ただし $(n,q-1)$ は n と $q-1$ の最大公約数.

［証 明］ （1） $|V(n+1,q)^*|=q^{n+1}-1$, $|[v]|=|GF(q)^*|=q-1$ より $|PG(n,q)|=(q^{n+1}-1)/(q-1)$ である．

（2），（3） $|Z(n,q)|=|GF(q)^*|=q-1$ より $|P\Gamma L(n,q)|=|\Gamma L(n,q)|/(q-1)$, $|PGL(n,q)|=|GL(n,q)|/(q-1)$ である．

（4） $SL(n,q)\cap Z(n,q)=\{\alpha\cdot 1\mid\alpha^n=1,\alpha\in GF(q)\}$ である．乗法群 $GF(q)^*$ は位数 $q-1$ の巡回群だから，$GF(q)^*=\langle\omega\rangle$ とおき $d=(n,q-1)$, $q-1=dl$ とする．

$\langle\omega^l\rangle$ は明らかに位数 d の巡回群で $(\omega^l)^n = \omega^{dl\cdot\frac{n}{d}} = \omega^{(q-1)\cdot\frac{n}{d}} = 1$ だから，$\langle\omega^l\rangle \subseteqq \{\alpha\in GF(q) \mid \alpha^n = 1\}$ である．逆に $\alpha^n = 1$ である $\alpha \in \langle\omega\rangle$ をとり $\alpha = \omega^r$ とする．$\alpha^n = \omega^{rn} = 1$ より $\omega^{\frac{n}{d}\cdot dr} = 1$ であり，$(n, q-1) = d$ より $\left(\frac{n}{d}, q-1\right) = 1$ であるから，$\omega^{\frac{n}{d}}$ は $\langle\omega\rangle$ の生成元である．したがって dr は $\langle\omega\rangle$ の位数 $q-1$ の倍数である．ここで $q-1 = dl$ より r は l の倍数となり $\alpha = \omega^r \in \langle\omega^l\rangle$ である．

以上より $SL(n,q)\cap Z(n,q) = \{\alpha\cdot 1 \mid \alpha\in\langle\omega^l\rangle\}$ となり，$|\langle\omega^l\rangle| = d$ より $|PSL(n,q)| = |SL(n,q)|/d$ となる．□

定 理 10.5 $PSL(n,K)$ $(n \geqq 2)$ は $PG(n-1, K)$ 上 2 重可移置換群である．

［証 明］ $PG(n-1,K)$ の異なる 2 点よりなる 2 つの組 $[v_1], [v_2]$ と $[u_1], [u_2]$ をとる．v_1, v_2 は 1 次独立であるから定理 1;5.4 より v_1, v_2 を含む基 $\{v_1, v_2, \cdots, v_n\}$ をもつ．同様に u_1, u_2 を含む $V(n, K)$ の基 $\{u_1, u_2, \cdots, u_n\}$ が存在する．注 9.5 より $v_i{}^a = u_i (i = 1, 2, \cdots, n)$ である $a\in GL(n, K)$ が存在する．$\det a = \alpha$ とする．

$GL(n,K)$ に $u_1{}^b = \alpha^{-1}u_1,\ u_i{}^b = u_i\ (i = 2, 3, \cdots, n)$ である元 b が存在し，$\det b = \alpha^{-1}$ である．このとき $\det ab = \det a\cdot\det b = \alpha\cdot\alpha^{-1} = 1$ となり，$ab \in SL(n, K)$ である．さらに $v_1{}^{ab} = \alpha^{-1}u_1, v_i{}^{ab} = u_i\ (i = 2, 3, \cdots, n)$ であるから

$$[v_1]^{[ab]} = [v_1{}^{ab}] = [\alpha^{-1}u_1] = [u_1],$$

$$[v_2]^{[ab]} = [v_2{}^{ab}] = [u_2]$$

となり，$PSL(n,K)$ は $PG(n-1,K)$ 上 2 重可移である．□

$V(n,K)$ のベクトルを座標で表して $v = (\lambda_1, \lambda_2, \cdots, \lambda_n)$ とするとき，$PG(n-1,K)$ の点として $[v] = [\lambda_1, \lambda_2, \cdots, \lambda_n]$ と表すこともある．このとき $\alpha\in K^\#$ に対して $[v] = [\alpha v]$ だから，$[\lambda_1, \lambda_2, \cdots, \lambda_n] = [\alpha\lambda_1, \alpha\lambda_2, \cdots, \alpha\lambda_n]$ である．

たとえば $PG(1,q)$ の点は，$GF(q)^\# = \langle\omega\rangle$ とすると $[0,1], [1,0], [1,1], [1,\omega], \cdots, [1,\omega^{q-2}]$ の $q+1$ 個よりなる．

定 理 10.6 $PGL(2,K)$ は $PG(1,K)$ 上 3 重可移置換群である．

［証 明］ $K = GF(q), GF(q)^\# = \langle\omega\rangle$ とし，$PG(1,K)$ の点を $[0,1], [1,0], [1,1], [1,\omega], \cdots, [1,\omega^{q-2}]$ とする．定理 10.5 より $PGL(2,K)$ は $PG(1,K)$ 上 2 重可移である．$PGL(2,K)$ における 2 点 $[0,1], [1,0]$ の安定化群を H とする．$\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\in H$ に対して

$$[0,1]^{\left[\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right]} = [\gamma, \delta] = [0,1]$$

より $\gamma=0, \delta\neq 0$ である．さらに

$$[1,0]^{\begin{bmatrix}\alpha & \beta \\ \gamma & \delta\end{bmatrix}}=[\alpha,\beta]=[1,0]$$

より $\alpha\neq 0,\ \beta=0$ である．したがって

$$\begin{bmatrix}\alpha & \beta \\ \gamma & \delta\end{bmatrix}=\begin{bmatrix}\alpha & 0 \\ 0 & \delta\end{bmatrix}=\begin{bmatrix}1 & 0 \\ 0 & \alpha^{-1}\delta\end{bmatrix}, \qquad \alpha^{-1}\delta\neq 0$$

である．逆に $\begin{bmatrix}1 & 0 \\ 0 & \lambda\end{bmatrix}$, $\lambda\neq 0$ は明らかに $[0,1],[1,0]$ を固定するから，$H=\left\{\begin{bmatrix}1 & 0 \\ 0 & \lambda\end{bmatrix} \middle| \lambda\in K^{\sharp}\right\}$ である．

$PG(1,q)-\{[0,1],[1,0]\}$ の任意の2点 $[1,\omega^i],[1,\omega^j]$ に対して $\begin{bmatrix}1 & 0 \\ 0 & \omega^{j-i}\end{bmatrix}\in H$ をとると

$$[1,\omega^i]^{\begin{bmatrix}1 & 0 \\ 0 & \omega^{j-i}\end{bmatrix}}=[1,\omega^j]$$

となり，Hは $PG(1,q)-\{[0,1],[1,0]\}$ 上可移である．したがって $PGL(2,K)$ は $PG(1,K)$ 上3重可移である．□

$K=GF(p^r)$（pは素数）とし，Ωを文字∞とKの元からなる集合 $\Omega=\{\infty\}\cup K$ とする．Ω からΩへの写像σを

$$\sigma:\xi\mapsto\frac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta} \qquad (\xi\in\Omega,\ \alpha,\beta,\gamma,\delta\in K,\ \alpha\delta-\beta\gamma\neq 0,\ \ i\text{ は整数})$$

により定義する．ただし $\xi\in K$ に対しては，$\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}$ は $\gamma\xi^{p^i}+\delta\neq 0$ のときKの演算によるKの元で，$\gamma\xi^{p^i}+\delta=0$ のときは∞とする．

また $\xi=\infty$ に対しては，写像σを $\gamma=0$ のとき$\infty\mapsto\infty$とし，$\gamma\neq 0$のとき$\dfrac{\alpha}{\gamma}$とする．

なおここで，写像 $\xi\mapsto\xi^{p^i}(\xi\in GF(p^r))$ は $GF(p^r)$ の自己同型で，特に自己同型が $GF(p^r)$ の恒等写像のとき，すなわち写像

$$\xi\mapsto\frac{\alpha\xi+\beta}{\gamma\xi+\delta} \qquad (\xi\in\Omega,\ \alpha,\beta,\gamma,\delta\in K,\ \alpha\delta-\beta\gamma\neq 0)$$

をΩ上の**1次分数変換**という．

補題 10.7 $K=GF(p^r)$（pは素数），$\Omega=\{\infty\}\cup GF(p^r)$ において写像 $\sigma:\Omega\to\Omega,\ \xi\mapsto\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}$ 全体の集合は，写像の積に関してΩ上の置換群を作り，1次分数変換全体の集合はその正規部分群になる．

［証明］ 写像 $\sigma:\xi\mapsto\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}$ はΩ上の置換であることをまず示す．

$\xi,\ \eta\in K$ に対して，$\xi^\sigma=\eta^\sigma$ とする．$\gamma\xi^{p^i}+\delta=0$ のとき $\xi^\sigma=\infty$ となり $\eta^\sigma=\infty$, $\gamma\eta^{p^i}+\delta=0$ である．ここで $\gamma=0$ とすると $\gamma\xi^{p^i}+\delta=0$ より $\delta=0$ になり $\alpha\delta-\beta\gamma\neq 0$ に反する．したがって $\gamma\neq 0$, $\xi^{p^i}=-\gamma^{-1}\delta=\eta^{p^i}$ となり，$\xi=\eta$ である．つぎに $\gamma\xi^{p^i}+\delta\neq 0$ とすると $\gamma\eta^{p^i}+\delta\neq 0$ で $\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}=\dfrac{\alpha\eta^{p^i}+\beta}{\gamma\eta^{p^i}+\delta}$ より

$$\alpha\gamma\xi^{p^i}\eta^{p^i}+\alpha\delta\xi^{p^i}+\beta\gamma\eta^{p^i}+\beta\delta=\alpha\gamma\xi^{p^i}\eta^{p^i}+\alpha\delta\eta^{p^i}+\beta\gamma\xi^{p^i}+\beta\delta$$

である．したがって $(\alpha\delta-\beta\gamma)(\xi-\eta)^{p^i}=0$ となり，$\alpha\delta-\beta\gamma\neq 0$ より $\xi=\eta$ である．

つぎに ∞^σ と ξ^σ $(\xi\in K)$ について考える．$\gamma=0$ のとき $\delta\neq 0$ で $\xi^\sigma=\delta^{-1}(\alpha\xi^{p^i}+\beta)$, $\infty^\sigma=\infty$ である．$\gamma\neq 0$ のとき $\infty^\sigma=\gamma^{-1}\alpha$ で一方 $\xi^\sigma=\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}=\dfrac{\alpha}{\gamma}$ とすると，$\alpha\gamma\xi^{p^i}+\beta\gamma=\alpha\gamma\xi^{p^i}+\alpha\delta$, $\alpha\delta-\beta\gamma=0$ になり仮定に反する．したがって $\xi^\sigma\neq\gamma^{-1}\alpha$ である．以上より σ は Ω 上の置換である．

2つの写像 $\xi\mapsto\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}$ と写像 $\xi\mapsto\dfrac{\alpha'\xi^{p^j}+\beta'}{\gamma'\xi^{p^j}+\delta'}$ の積は $\xi\mapsto\dfrac{\alpha''\xi^{p^{i+j}}+\beta''}{\gamma''\xi^{p^{i+j}}+\delta''}$ になり，$\alpha''\delta''-\beta''\gamma''\neq 0$ をみたすことはみやすい．

また Ω 上恒等写像になるのは写像 $\xi\mapsto\xi$ に限る．したがって写像 $\xi\mapsto\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}$ の全体は Ω 上の置換群になる．ここで写像 $\xi\mapsto\dfrac{\alpha\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\delta}$ の逆写像は $\xi\mapsto\dfrac{\delta^{p^{-i}}\xi^{p^{-i}}-\beta^{p^{-i}}}{-\gamma^{p^{-i}}\xi^{p^{-i}}+\alpha^{p^{-i}}}$ であり，これより1次分数変換全体の集合は正規部分群になることは容易にたしかめられる．□

$K=GF(q),\ q=p^r$ とする．補題10.7で作られた $\Omega=\{\infty\}\cup K$ 上の置換群を $\Gamma F(K)$ または $\Gamma F(q)$ と書くことにする．特に1次分数変換全体の作る群を**1次分数変換群**といい，$LF(K)$ または $LF(q)$ と書く．

定理 10.8 置換群として

$$(P\Gamma L(2,K),PG(1,K))\cong(\Gamma F(K),\Omega),$$
$$(PGL(2,K),PG(1,K))\cong(LF(K),\Omega)$$

である．ここで $\Omega=\{\infty\}\cup K$ である．

［証 明］ $K=GF(p^r)$（p は素数）とする．対応 $[0,1]\leftrightarrow\infty$, $[1,\xi]\leftrightarrow\xi$ $(\xi\in K)$ により $PG(1,K)$ と Ω の間の1対1対応がえられる．

$\mathrm{Aut}\,GF(p^r)=\langle\theta\rangle$, $\theta^i:\xi\mapsto\xi^{p^i}$ $(\xi\in K)$ とすると，定理 9.10 より $P\Gamma L(2,K)$ の元 $[\theta^i]$ が $[\xi,\eta]^{[\theta^i]}=[\xi^{p^i},\eta^{p^i}]([\xi,\eta]\in PG(1,K))$ により定義できる．さらに定理 9.10 より $P\Gamma L(2,K)=\langle[\theta]\rangle\cdot PGL(2,K)$ で，$\langle[\theta]\rangle\cap PGL(2,K)=1$ より $P\Gamma L(2,K)$

の元は $[\theta^i]\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$, $\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}\in PGL(2,K)$ と一意的に書ける.

一方 $\Gamma F(K)$ の元 $\xi\mapsto\dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}$ において, $\alpha\delta-\beta\gamma\neq 0$ で任意の $\lambda\in K^\#$ に対して $\dfrac{\lambda\delta\xi^{p^i}+\lambda\beta}{\lambda\gamma\xi^{p^i}+\lambda\alpha}=\dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}$ であるから, $[\theta^i]\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$ と $\xi\mapsto\dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}$ を対応させると, $P\Gamma L(2,K)$ と $\Gamma F(K)$ の間の1対1対応がえられる.

この対応において

$$[0,1]^{[\theta^i]\left[\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right]}=[\gamma,\delta]=\begin{cases}[0,1] & ;\ \gamma=0\ のとき\\ [1,\gamma^{-1}\delta]; & \gamma\neq 0\ のとき\end{cases}$$

である. 一方 $\xi\mapsto\dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}$ により

$$\infty\mapsto\begin{cases}\infty & ;\ \gamma=0\ のとき\\ \gamma^{-1}\delta; & \gamma\neq 0\ のとき\end{cases}$$

である. つぎに $\xi\in K$ に対して

$$[1,\xi]^{[\theta^i]\left[\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right]}=[1,\xi^{p^i}]^{\left[\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right]}=[\alpha+\gamma\xi^{p^i},\beta+\delta\xi^{p^i}]$$

$$=\begin{cases}[0,1]\,; & \alpha+\gamma\xi^{p^i}=0\ のとき\\ \left[1,\dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}\right]; & \alpha+\gamma\xi^{p^i}\neq 0\ のとき\end{cases}$$

である. 一方 $\xi\mapsto\dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}$ により

$$\xi\mapsto\begin{cases}\infty\,; & \alpha+\gamma\xi^{p^i}=0\ のとき\\ \dfrac{\delta\xi^{p^i}+\beta}{\gamma\xi^{p^i}+\alpha}; & \alpha+\gamma\xi^{p^i}\neq 0\ のとき\end{cases}$$

である.

以上より $P\Gamma L(2,K)$ と $\Gamma F(K)$ の対応する元による置換は $PG(1,K)$ と Ω との間の対応を保ち, $(P\Gamma L(2,K),PG(1,K))\cong(\Gamma F(K),\Omega)$ である.

さらにこの対応において $\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$ と $\xi\mapsto\dfrac{\delta\xi+\beta}{\gamma\xi+\alpha}$ が対応するから, $(PGL(2,K),PG(1,K))\cong(LF(K),\Omega)$ である. □

系 10.9 $K=GF(q)$, $K^\#=\langle\omega\rangle$ とし, $PSL(2,K)$ に対応する $LF(K)$ の部分群を $L_2(K)$ とおく. このとき

$$LF(K)=\langle\xi\mapsto-\xi^{-1},\xi\mapsto\xi+1,\xi\mapsto\omega\xi\rangle,$$
$$L_2(K)=\langle\xi\mapsto-\xi^{-1},\xi\mapsto\xi+1,\xi\mapsto\omega^2\xi\rangle$$

である.

[証 明] 定理 10.6 および定理 10.8 より $LF(K)$ は $\Omega=\{\infty,0,1,\omega,\cdots,\omega^{q-2}\}$ 上 3重可移で, 定理 10.4 より $|LF(K)|=(q+1)q(q-1)$ である. ここで

$$\xi \mapsto -\xi^{-1} = (\infty\ 0)\cdots$$
$$\xi \mapsto \xi + 1 = (\infty)(0\ 1\ \cdots)\cdots$$
$$\xi \mapsto \omega\xi = (\infty)(0)(1\ \omega\ \cdots\ \omega^{q-2})$$

であるから，$\langle(\infty\ 0)\cdots, (\infty)(0\ 1\ \cdots)\cdots, (\infty)(0)(1\ \omega\ \cdots\ \omega^{q-2})\rangle$ はΩ上3重可移になり，位数より $LF(K)$ に一致する．

定理 10.8 の $PGL(2,K)$ と $LF(K)$ の対応において

$$\xi \mapsto -\xi^{-1} \leftrightarrow \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$
$$\xi \mapsto \xi + 1 \leftrightarrow \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$
$$\xi \mapsto \omega^2\xi = \frac{\omega\xi}{\omega^{-1}} \leftrightarrow \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix}$$

であるから，$\xi \mapsto -\xi^{-1}$, $\xi \mapsto \xi+1$, $\xi \mapsto \omega^2\xi$ は $L_2(K)$ の元である．さらに $|L_2(K)| = |LF(K)|/(2, q-1)$ であるから，q が 2 のべきのとき $LF(K) = L_2(K)$ で $K^\sharp = \langle\omega^2\rangle$ より，これらは $L_2(K)$ の生成元である．つぎに q が奇数のとき $|L_2(K)| = |LF(K)|/2$ で，定理 10.4 より $L_2(K)$ はΩ上2重可移である．また

$$\xi \mapsto \omega^2\xi = (\infty)(0)(1\ \omega^2\ \cdots\ \omega^{q-3})(\omega\ \omega^3\ \cdots\ \omega^{q-2})$$

であるから，$\langle\xi \mapsto -\xi^{-1}, \xi \mapsto \xi+1, \xi \mapsto \omega^2\xi\rangle$ はΩ上2重可移で，位数より $L_2(K)$ に一致する．□

定理 10.10 $PSL(n,q)$ は $PSL(2,2)$, $PSL(2,3)$ を除き単純群である．

［証明］ $V = V(n,q)$ の基を $\{v_1, v_2, \cdots, v_n\}$ とし，$G = PSL(n,q)$, $(n,q) \neq (2,2), (2,3)$ とおく．Gは定理 10.5 より $PG(n-1,q)$ 上2重可移である．

いまGは単純でないと仮定し，NをGの極大な正規部分群とする．系 7.9 よりNは $PG(n-1,q)$ 上可移で，したがって $G = G_{[v_1]}N$ である．ここで

$$G_{[v_1]} = \left\{\begin{bmatrix} \alpha & 0 & \cdots & 0 \\ & * & & \end{bmatrix} \in G\right\}$$

である．

定理 9.2 より $SL(n,q) = \langle a_{i,j}(\alpha) \mid i,j = 1,2,\cdots,n,\ \alpha \in GF(q)\rangle$

$$a_{i,j}(\alpha) = \begin{pmatrix} 1 & & \vdots^{\,j} & & \\ & 1 & \vdots & 0 & \\ & & \ddots & & \\ \cdots & \cdots & \alpha & \ddots & \cdots \\ & & \vdots & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ i) \\ \\ \end{matrix}$$

である．いま $H = \langle[a_{i,1}(\alpha)] \mid i = 2, 3, \cdots, n,$

$\alpha\in GF(q)\rangle$ とおくと，$H\leqq G_{[v_1]}$ である．

任意の $v=\sum_{i=1}^{n}\lambda_i(v)\cdot v_i$ に対して $v^{a_{i,1}(\alpha)}=v+\alpha\cdot\lambda_i(v)\cdot v_1$ であるから

$$v^{a_{i,1}(\alpha)\cdot a_{j,1}(\beta)}=(v+\alpha\cdot\lambda_i(v)\cdot v_1)^{a_{j,1}(\beta)}=v+\alpha\cdot\lambda_i(v)v_1+\beta\cdot\lambda_j(v)\cdot v_1$$
$$=v^{a_{j,1}(\beta)\cdot a_{i,1}(\alpha)}$$

となり

$$a_{i,1}(\alpha)\cdot a_{j,1}(\beta)=a_{j,1}(\beta)\cdot a_{i,1}(\alpha),$$
$$[a_{i,1}(\alpha)]\ [a_{j,1}(\beta)]=[a_{j,1}(\beta)]\ [a_{i,1}(\alpha)]$$

が成り立ち，したがってHは可換群である．

任意の $a\in SL(n,q)$，任意の $v=\sum_{i=1}^{n}\lambda_i(v)v_i\in V$ に対して

$$v^{a^{-1}\cdot a_{i,1}(\alpha)\cdot a}=(v^{a^{-1}})^{a_{i,1}(\alpha)\cdot a}=(v^{a^{-1}}+\alpha\cdot\lambda_i(v^{a^{-1}})\cdot v_1)^a=v+\alpha\cdot\lambda_i(v^{a^{-1}})\cdot {v_1}^a$$

である．いま $a=\begin{pmatrix}\alpha_{11}\ 0\cdots 0\\ *\end{pmatrix}$, $[a]\in G_{[v_1]}$ とすると $a^{-1}=(\alpha'_{ij})=\begin{pmatrix}{\alpha_{11}}^{-1}\ 0\cdots 0\\ *\end{pmatrix}$

$$v^{a^{-1}\cdot a_{i,1}(\alpha)\cdot a}=v+\alpha\cdot\lambda_i(v^{a^{-1}})\cdot {v_1}^a=v+\alpha\cdot(\sum_{j=1}^{n}\lambda_j(v)\alpha'_{ji})\cdot\alpha_{11}\cdot v_1$$
$$=v+\sum_{j=2}^{n}\alpha\cdot\alpha_{11}\cdot\alpha'_{ji}\cdot\lambda_j(v)\cdot v_1=v^{\bar a},\qquad \bar a=\prod_{j=2}^{n}a_{j,1}(\alpha\alpha_{11}\alpha'_{ji})$$

である．したがって $a^{-1}\cdot a_{i,1}(\alpha)\cdot a=\prod_{j=2}^{n}a_{j,1}(\alpha\alpha_{11}\alpha'_{ji})$, $[a]^{-1}\cdot[a_{i,1}(\alpha)]\ [a]\in H$ となり，$G_{[v_1]}\geqq H$ である．さらに $G=G_{[v_1]}N, G\geqq N$ より，$G\geqq HN$ となる．ここでNはGの極大正規部分群であるから，$G=HN$ または $N\geqq H$ である．

いま $N\geqq H$ とする．
$$a_k=\begin{pmatrix}0 & & & 1 & & & \\ & 1 & & \vdots & & & \\ & & \ddots & \vdots & & & \\ & & & 1\ \vdots & & & \\ -1 & \cdots & \cdots & 0 & \cdots & \cdots & \\ & & & \vdots & 1 & & \\ & & & \vdots & & \ddots & \\ & & & \vdots & & & 1\end{pmatrix}\ (k\text{列目})$$
$\in SL(n,q)$, $(k=2,3,\cdots,n)$ をとると
$$a_k^{-1}=\begin{pmatrix}0 & & & -1 & & & \\ & 1 & & \vdots & & & \\ & & \ddots & \vdots & & & \\ & & & 1\ \vdots & & & \\ 1 & \cdots & \cdots & 0 & \cdots & \cdots & \\ & & & \vdots & 1 & & \\ & & & \vdots & & \ddots & \\ & & & \vdots & & & 1\end{pmatrix}\ (k\text{列目})$$
である．ここでa_kは単位

行列の1列とk列を入れかえて，$(k,1)$ 成分を -1にしたものである．このとき任意の$v=\sum_{i=1}^{n}\lambda_i(v)v_i\in V$ に対して

$$
\begin{aligned}
v^{a_k^{-1}\cdot a_{i,1}(\alpha)\cdot a_k} &= v+\alpha\cdot\lambda_i(v^{a_k^{-1}})\cdot v_1{}^{a_k} \\
&= \begin{cases} v+\alpha\cdot\lambda_i(v)\cdot v_k = v^{a_{i,k}(\alpha)} & (i\neq k \text{ のとき}) \\ v+\alpha\cdot(-\lambda_1(v))\cdot v_k = v^{a_{1,i}(\alpha)^{-1}} & (i=k \text{ のとき}) \end{cases}
\end{aligned}
$$

となり，したがって$i\neq k$のとき $a_k{}^{-1}a_{i,1}(\alpha)a_k=a_{i,k}(\alpha)$ で，$a_i{}^{-1}a_{i,1}(\alpha)a_i=a_{1,i}(\alpha)^{-1}$ $(i,k=2,3,\cdots,n)$ となる．ここで $[a_{i,1}(\alpha)]\in N$ で，$N\lhd G$ よりNは $[a_{i,j}(\alpha)]$$(i,j=1,2,\cdots,n,\ \alpha\in GF(q))$ をすべて含み，定理 9.2 よりこれらの元によりGが生成されるから $G=N$ となり仮定に反する．

つぎに $G=HN$ とする．このとき定理 1;3.3 より $G/N=HN/N\cong H/(H\cap N)$ となり，Hは可換群であるから G/N も可換群になり，定理 1;4.1 よりNはGの交換子群$D(G)$ を含む．

一方系 9.3 より $SL(n,q)$ は $SL(2,2), SL(2,3)$ を除き，その交換子群 $D(SL(n,q))$ に等しい．いま $Z=Z(n,q)\cap SL(n,q)$ とおくと

$$
\begin{aligned}
D(PSL(n,q)) &= D(SL(n,q)/Z) = D(SL(n,q))\cdot Z/Z \\
&= SL(n,q)/Z = PSL(n,q)
\end{aligned}
$$

より $N=G$ となり仮定に反する．

以上より $G=PSL(n,q)$ は単純群である．□

補 題 10.11 $PSL(2,2)\cong S_3$, $PGL(2,3)\cong S_4$, $PSL(2,3)\cong A_4$ である．

［証 明］ $|PG(1,2)|=(2^2-1)/(2-1)=3$, $|PSL(2,2)|=(2^2-1)(2^2-2)/(2-1)(2,1)=3\cdot 2$ であるから，$PSL(2,2)$ は $PG(1,2)$ 上対称群 S_3 である．

$|PG(1,3)|=(3^2-1)/(3-1)=4$ で，$|PGL(2,3)|=(3^2-1)(3^2-3)/(3-1)=24$, $|PSL(2,3)|=|PGL(2,3)|/(2,2)=12$ である．したがって $PGL(2,3)$ は $PG(1,3)$ 上対称群 S_4 であり，$PSL(2,3)$ は S_4 の指数2の正規部分群として補題 3.11 (2) より交代群 A_4 である．□

補 題 10.12 $PSL(2,4)\cong PSL(2,5)\cong A_5$, $PGL(2,5)\cong S_5$ である．

［証 明］ $|PG(1,4)|=5$ で，$|PSL(2,4)|=60$ である．したがって $PSL(2,4)$ は5次の置換群として対称群 S_5 の指数2の部分群となり，補題 3.11 (1) より A_5 に一致する．

$|PG(1,5)|=6$で，$|PGL(2,5)|=120$ である．定理 10.8 より $(PGL(2,5), PG(1,5))$ を $(LF(5), \{\infty\}\cup GF(5))$, $GF(5)=\{0,1,2,3,4\}$ として考える．

$LF(5)$ の元 $a:\xi\mapsto\xi+1$, $b:\xi\mapsto\dfrac{2}{\xi}$ をとると

$$a=(\infty)(0\ \ 1\ \ 2\ \ 3\ \ 4),$$
$$b=(\infty\ \ 0)(1\ \ 2)(3\ \ 4)$$

である．注 6.10 の証明で示したように，$\langle a,b\rangle$ は6次の置換群としての対称群 S_5 に一致する．一方 $|PGL(2,5)|=|S_5|$ であるから，6次の置換群として $PGL(2,5)$ と S_5 は同型である．

$PSL(2,5)$ は $PGL(2,5)$ の指数2の部分群であるから，補題 3.11（1）より交代群 A_5 と同型である．□

補 題 10.13 $PSL(2,9)\cong A_6$ である．

［**証 明**］ $|PSL(2,9)|=|A_6|=360$ である．いま定理 10.8 および系 10.9 を用いて $(PSL(2,9), PG(1,9))$ を $(L_2(9), \{\infty\}\cup GF(9))$ として考え，ω を $\omega^2=2\omega+1$ をみたす $GF(9)^\sharp$ の生成元とする．したがって $\omega^3=2\omega+2$, $\omega^4=2$, $\omega^5=2\omega$, $\omega^6=\omega+2, \omega^7=\omega+1$ である．

$LF(9)$ の元 $\xi\mapsto\dfrac{\alpha\xi+\beta}{\gamma\xi+\delta}$ において $\dfrac{\alpha\xi+\beta}{\gamma\xi+\delta}=\dfrac{\lambda\alpha\xi+\lambda\beta}{\lambda\gamma\xi+\lambda\delta}$ $(\lambda\in GF(9)^\sharp)$ であるから $\xi\mapsto\dfrac{\alpha\xi+\beta}{\gamma\xi+\delta}$ が $L_2(9)$ の元であるためには，対応する $PSL(2,9)$ の元 $\begin{bmatrix}\lambda\delta & \lambda\beta\\ \lambda\gamma & \lambda\alpha\end{bmatrix}$ をとることにより，$\det\begin{bmatrix}\lambda\delta & \lambda\beta\\ \lambda\gamma & \lambda\alpha\end{bmatrix}=\lambda^2(\alpha\delta-\beta\gamma)=1$ をみたす $\lambda\in GF(9)^\sharp$ が存在すればよい．すなわち $(\alpha\delta-\beta\gamma)\in\{1,\omega^2,\omega^4,\omega^6\}$ であればよい．

$\Delta_1=\{\infty\}\cup GF(3)=\{\infty,0,1,\omega^4\}$ とおき，$L_2(9)$ の元 $a:\xi\mapsto\dfrac{\omega\xi+1}{\xi}$ をとる．

$$a=(\infty\ \ \omega\ \ \omega^2\ \ \omega^3\ \ 0)(1\ \ \omega^7\ \ \omega^5\ \ \omega^4\ \ \omega^6)$$

である．このとき

$$\Delta_2=\Delta_1{}^a=\{\omega,\infty,\omega^7,\omega^6\}$$
$$\Delta_3=\Delta_2{}^a=\{\omega^2,\omega,\omega^5,1\}$$
$$\Delta_4=\Delta_3{}^a=\{\omega^3,\omega^2,\omega^4,\omega^7\}$$
$$\Delta_5=\Delta_4{}^a=\{0,\omega^3,\omega^6,\omega^5\}$$

とおき $\Omega=\{\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_5\}$ とすると，a は Ω 上の置換として

$$\bar{a}=(\Delta_1\ \Delta_2\ \Delta_3\ \Delta_4\ \Delta_5)$$

と書ける．つぎに $L_2(9)$ の元 $b:\xi\mapsto\xi+1$ をとると

$$b=(\infty)(0\ \ 1\ \ \omega^4)(\omega\ \ \omega^7\ \ \omega^6)(\omega^2\ \ \omega^3\ \ \omega^5)$$

で，b は Ω 上の置換 $\bar{b}$ を導き

$$\bar{b}=(\Delta_1)\ (\Delta_2)\ (\Delta_3\ \Delta_4\ \Delta_5)$$

となる．このとき明らかに $\langle\bar{a},\bar{b}\rangle$ はΩ上の交代群 A_5 になり，$\langle a,b\rangle$ はΩ上 A_5 として置換表現される．いまこの置換表現の核の元xをとる．任意の $\lambda\in\{\infty\}\cup GF(9)$ に対して，異なるちょうど2つの Δ_i, Δ_j がΩに存在して，$\{\lambda\}=\Delta_i\cap\Delta_j$ であるから，$\{\lambda^x\}=\Delta_i^x\cap\Delta_j^x=\Delta_i\cap\Delta_j=\{\lambda\}$ となり $x=1$ である．したがって $\langle a,b\rangle$ は A_5 に同型になる．

このとき $|L_2(9):\langle a,b\rangle|=6$ より，$(L_2(9),\ L_2(9)/\langle a,b\rangle)$ は6次の置換群となる．また定理 10.10 より $L_2(9)$ は単純群であるから，この置換表現は忠実である．以上より $PSL(2,9)$ は6次の忠実な置換表現をもち，$|PSL(2,9)|=|S_6|/2$ であるから，A_6 に同型になる．□

さらにつぎの同型も成り立つ．

$$PSL(4,2)\cong A_8,\qquad PSL(2,7)\cong PSL(3,2).$$

ここで $PSL(4,2)=PGL(4,2)\cong GL(4,2)$ であるが，これが A_8 と同型であることは，第3章 §1 で示す．

問 10.1　$PSL(n,p^r)$ において，$H=\left\{\begin{bmatrix}1 & & 0\\ & \ddots & \\ * & & 1\end{bmatrix}\right\}$は p-シロー部分群であり，さらに $PGL(n,p^r)$ の p-シロー部分群でもあることを示せ．

問 10.2　$PGL(V)$ の元が同一直線上にある $PG(V)$ の3点を固定すれば，この元はこの直線上のすべての点を固定することを示し，このことは $P\Gamma L(V)$ の元についてはいえないことを示せ．

問 10.3　Ω上の t 重可移群Gが，$G_{12\cdots t}=1$ のときGを**強 t 重可移群**という．$PGL(2,K)$ は $PG(1,K)$ 上強3重可移であることを示せ．

問 10.4　$PG(1,q)$ 上の置換群 $G=PSL(2,q)$ において，HをGにおける2点の安定化群とする．このときHは位数 $(q-1)/(2,\ q-1)$ の巡回群で，$N_G(H)$ は位数 $2\cdot|H|$ の2面体群であることを示せ．

§11. 半正則，正則

Ω上の置換群Gが，すべての $i\in\Omega$ に対して $G_i=1$ のとき，Gを**半正則** (semiregular) という．なお $G=1$ のときも定義より半正則である．

またΩ上の置換群が，Ω上可移でかつ半正則のとき，**正則** (regular) という．GがΩ上可移群のとき，$G_i=1$ となる $i\in\Omega$ があれば，すべての $i\in\Omega$

に対して $G_i=1$ となり，Gは正則である.

定理 11.1 GをΩ上の置換群とする.

(1) Gが半正則であることと，G-軌道の長さがすべて $|G|$ に等しいこととは同値である.

(2) したがってGが正則であれば $|G|=|\Omega|$ である.

［証明］ 任意の $i\in\Omega$ に対して $|G|=|G_i|\cdot|i^G|$ である. したがって $|G_i|=1$ のときそのときに限り $|G|=|i^G|$ である. これよりGが半正則であることと，すべての i に対して $|G|=|i^G|$ であることとは同値である.

特にGが正則であれば $\Omega=i^G$ であるから，$|G|=|\Omega|$である. □

系 11.2 Gを群, HをGの部分群とする. Gの部分群Hによる置換表現において，HがGの正規部分群であるときそのときに限り $(G, G/H)$ は正則である.

［証明］ Gの部分群Hによる置換表現をφとする. 定理 6.3 より G^φ は G/H 上可移である. したがって定理 11.1 より $|G^\varphi|=|G/H|$ のときそのときに限り G^φ は正則である.

一方定理 6.3 より $\ker\varphi=\bigcap_{x\in G} H^x \leqq H$ であるから，$|G^\varphi|=|G/\ker\varphi|\geqq|G/H|$ である. したがって

$$G^\varphi \text{ が正則} \Longleftrightarrow |G/\ker\varphi|=|G/H| \Longleftrightarrow \ker\varphi=H \Longleftrightarrow H\trianglelefteq G$$

である. □

定理 11.3 GをΩ上の置換群とする. このときGが正則であることと，任意の $i\in\Omega$ に対して $1^a=i$ なる元aがGにただ1つ存在することとは同値である.

［証明］ Gを正則とする. Gは Ω 上可移だから任意の $i\in\Omega$ に対して $1^a=i$ なる $a\in G$ が存在する. いま $1^a=1^{a'}=i, a'\in G$ とすると $1^{aa'^{-1}}=1, aa'^{-1}\in G_1=1$ となり $a=a'$ である.

逆に任意の $i\in\Omega$ に対して $1^a=i$ なる元aがGにただ1つ存在するとする. 定理2.3よりGはΩ上可移であり，$G_1=\{x\in G\mid 1^x=1\}=1$ であるからGは正則である. □

定理 11.3 を用いてつぎのことがいえる.

注 11.4 GがΩ上正則のとき，$G=\{a_1, a_2, \cdots, a_n\}$ とすると $\Omega=\{1^{a_1}, 1^{a_2}, \cdots, 1^{a_n}\}$ である.

系 11.5 以下系11.10までΩ上の対称群をSと書くことにする．GをΩ上正則な置換群とし，$a\in N_S(G)$ とする．いまaの固定点集合を $F(a)=\{1,2,\cdots,k\}(k\geqq 1)$ とすると，$C_G(a)=\{a_i\in G\,|\,1^{a_i}=i,\,i=1,2,\cdots,k\}$ で位数kである．

［証 明］ Gは正則だから，定理 11.3 より $1^{a_i}=i$ ($i=1,2,\cdots,k$) となる $a_i\in G$ がただ1つ存在する．このとき $1^{a^{-1}a_ia}=1^{a_ia}=i^a=i$ で $a\in N_S(G)$ より $a_i{}^a\in G$ であるから，$a_i{}^a=a_i$, $a_i\in C_G(a)$ である．

逆に $x\in C_G(a)$ とすると，$F(a)^x=F(a^x)=F(a)$ である．したがって $1^x=i\in F(a)$ となり $x=a_i$ である．以上より，$C_G(a)=\{a_1,a_2,\cdots,a_k\}$ である．□

定 理 11.6 GをΩ上正則な置換群，したがって $G=\{a_1,a_2,\cdots,a_n\}$, $\Omega=\{1^{a_1},1^{a_2},\cdots,1^{a_n}\}$ とする．

（1） $C_S(G)=\{a_i'\,|\,a_i\in G\}$, $a_i'=\begin{pmatrix}1^{a_1} & 1^{a_2} & \cdots & 1^{a_n}\\ 1^{a_i{}^{-1}a_1} & 1^{a_i{}^{-1}a_2} & \cdots & 1^{a_i{}^{-1}a_n}\end{pmatrix}$ である．

（2） (G,Ω) と $(C_S(G),\Omega)$ は対応 $a_i\leftrightarrow a_i'$, $1^{a_i}\leftrightarrow 1^{a_i{}^{-1}}$ ($i=1,2,\cdots,n$) により同値な置換群である．

［証 明］ $G'=\{a_i'\,|\,a_i\in G\}$ とおく．a_i' はΩ上の置換で，$i\neq j$ であれば $a_i'\neq a_j'$ である．

（1） 任意の $a_k\in G$, $a_l'\in G'$ をとる．任意の $1^{a_i}\in\Omega$ に対して

$$(1^{a_i})^{a_ka_l'}=(1^{a_ia_k})^{a_l'}=1^{a_l{}^{-1}a_ia_k}=(1^{a_i})^{a_l'a_k}$$

であるから，$a_ka_l'=a_l'a_k$ となり $G'\subseteqq C_S(G)$ である．

逆に任意の $x\in C_S(G)$ をとる．GはΩ上可移であるから，$1^{xa_l}=1$ である $a_l\in G$ が存在する．このとき任意の $1^{a_i}\in\Omega$ に対して

$$(1^{a_i})^x=1^{xa_i}=1^{a_l{}^{-1}a_i}=(1^{a_i})^{a_l'}$$

となり，$x=a_l'\in G'$, $G'=C_S(G)$ である．

（2） (G,Ω) から $(C_S(G),\Omega)$ への写像をつぎのように定義する．

$$\text{写像 } \varphi\colon \Omega\to\Omega,\ 1^{a_i}\mapsto 1^{a_i{}^{-1}}$$

$$\text{写像 } f\colon G\to C_S(G),\ a_i\mapsto a_i'$$

このとき明らかに φ, f は全単射である．

任意の $1^{a_i}\in\Omega$, 任意の $a_k\in G$ に対して

$$((1^{a_i})^{a_k})^\varphi=(1^{a_ia_k})^\varphi=1^{(a_ia_k)^{-1}}=1^{a_k{}^{-1}a_i{}^{-1}},$$

$$((1^{a_i})^\varphi)^{a_k'}=(1^{a_i{}^{-1}})^{a_k'}=1^{a_k{}^{-1}a_i{}^{-1}}$$

より $((1^{a_i})^{a_k})^\varphi=((1^{a_i})^\varphi)^{a_k'}$ が成り立ち，$(G,\Omega)\cong(C_S(G),\Omega)$ である．□

群Gの単位群1による左置換表現を**左正則表現**という．いま $G=\Omega=\{a_1, a_2, \cdots, a_n\}$ とし，$*G=\{*a_i \mid a_i \in G\}$，$*a_i=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i^{-1}a_1 & a_i^{-1}a_2 & \cdots & a_i^{-1}a_n \end{pmatrix}$とするとき，左正則表現による置換群は $(*G, \Omega)$ である．

系 11.7 群Gの右および左正則表現による置換群をそれぞれ (G^*, Ω)，$(*G, \Omega)$ とすると $C_S(G^*)=*G$ である．

［証 明］ $G=\{a_1, a_2, \cdots, a_n\}=\Omega$ とすると，$G^*=\{a_i^* \mid a_i \in G\}$，

$a_i^*=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1a_i & a_2a_i & \cdots & a_na_i \end{pmatrix}$ で，$*G$は上の通りとする．いまGの単位元1により $a_i=1\cdot a_i=1^{a_i^*}$ であるから $\Omega=\{1^{a_1^*}, 1^{a_2^*}, \cdots, 1^{a_n^*}\}$ である．このとき定理 11.6 より

$C_S(G^*)=\{(a_i^*)' \mid a_i^* \in G^*\}$

$$(a_i^*)'=\begin{pmatrix} 1^{a_1^*} & 1^{a_2^*} & \cdots & 1^{a_n^*} \\ 1^{a_i^{*-1}\cdot a_1^*} & 1^{a_i^{*-1}\cdot a_2^*} & \cdots & 1^{a_i^{*-1}\cdot a_n^*} \end{pmatrix}=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i^{-1}a_1 & a_i^{-1}a_2 & \cdots & a_i^{-1}a_n \end{pmatrix}=*a_i$$

となり，$C_S(G^*)=*G$ である．□

つぎは定理 11.6 よりただちにえられる．

系 11.8 GをΩ上正則な可換群とすれば，$C_S(G)=G$ である．

定 理 11.9 GをΩ上の置換群とする．このとき，GがΩ上半正則であることと $C_S(G)$ がΩ上可移であることとは同値である．

［証 明］ $C_S(G)$ がΩ上可移とする．いま $F(x) \neq \phi$ である $x \in G$ をとると，xと $C_S(G)$ の元は可換であるから $F(x)^{C(G)}=F(x)$ である．ここで $C_S(G)$ はΩ上可移であるから，$F(x)^{C(G)}=\Omega$ すなわち $F(x)=\Omega$ となり $x=1$ である．したがって Gは半正則である．

逆にGがΩ上半正則とする．いま G-軌道を $\Delta_1, \Delta_2, \cdots, \Delta_r$ とし，各 Δ_k より1文字ずつ $i_1, i_2, \cdots, i_r$ $(i_k \in \Delta_k)$ をえらぶ．$G=\{a_1, a_2, \cdots, a_m\}$ とすると，G^{Δ_k} は Δ_k 上正則で $G \cong G^{\Delta_k}$ であるから，注 11.4 より $\Delta_k=\{i_k^{a_1}, i_k^{a_2}, \cdots, i_k^{a_m}\}$，$|\Omega|=|G|\cdot r$ である．Ω上の置換

$$c=(i_1^{a_1}\ i_2^{a_1}\ \cdots\ i_r^{a_1})(i_1^{a_2}\ i_2^{a_2}\ \cdots\ i_r^{a_2})\cdots(i_1^{a_m}\ i_2^{a_m}\ \cdots\ i_r^{a_m})$$

をとると，右辺はcの巡回表示でΩ上に固定点をもたない．さらに $\langle c\rangle$ は G-軌道の集合 $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ 上可移に作用するから，$\langle G, c\rangle$ はΩ上可移である．任意の $x \in G$ に対して

$$c^x=(i_1^{a_1x}\ i_2^{a_1x}\ \cdots\ i_r^{a_1x})(i_1^{a_2x}\ i_2^{a_2x}\ \cdots\ i_r^{a_2x})\cdots(i_1^{a_mx}\ i_2^{a_mx}\ \cdots\ i_r^{a_mx})$$

で，$\{a_1, a_2, \cdots, a_m\}=\{a_1x, a_2x, \cdots, a_mx\}$ であるから $c^x=c$ となり，cはGのすべての

元と可換である. したがって$G\cap\langle c\rangle=1$より, $\langle G,c\rangle=G\times\langle c\rangle$, $|\langle G,c\rangle|=|G|\cdot|\langle c\rangle|=|G|\cdot r=|\Omega|$ となり, 定理 11.1 より $\langle G,c\rangle$ はΩ上正則である.

以上より, 定理 11.6 を用いて $C_S(\langle G,c\rangle)$ はΩ上可移で, $C_S(\langle G,c\rangle)\leqq C_S(G)$ より $C_S(G)$ もΩ上可移である. □

系 11.10 GをΩ上可移である置換群とする. このときGは可換群であれば正則である.

［**証 明**］ Gは可換群だから, $G\leqq C_S(G)$ である. ここでGは可移だから $C_S(G)$ も可移で, 定理 11.9 よりGは半正則になり, したがって正則である. □

Ω上の置換群Gがつぎの3つの条件をみたすとき, Gを **Frobenius 群**という.

（1） GはΩ上可移である.

（2） Gは正則ではない（すなわち$G_i\neq 1$).

（3） G_i は $\Omega-\{i\}$ 上半正則である（すなわち任意の $i,j(\neq)\in\Omega$ に対して $G_{ij}=1$).

Gを Frobenius 群とするとき, G_iをGの **Frobenius 補群**, $\{x\in G\,|\,F(x)=\phi\}\cup\{1\}$ をGの **Frobenius 核**という.

Frobenius 群の例： （i） 3次対称群 S_3, 4次交代群 A_4 および奇数n次の2面体群 D_{2n} は Frobenius 群である.

（ii）$\Omega=\{\infty\}\cup GF(q)$ 上の置換群 $LF(q)$ において, 1点∞における安定化群をGとすると

$$G=\{a_{\alpha,\beta}\in LF(q)\,|\,a_{\alpha,\beta};\xi\mapsto\alpha\xi+\beta,\ \alpha(\neq 0),\beta,\xi\in GF(q)\}$$

である. このとき定理 10.6 および定理 10.8 よりGは $q>2$ のとき $GF(q)$ 上の2重可移群で $G_0=\{a_{\alpha,0}\}\neq 1, G_1=\{a_{\alpha,1-\alpha}\}\neq 1$ である. したがって $G_{0\,1}=G_0\cap G_1=\{a_{1,0}\}=1$ となりGは Frobenius 群である. このとき Frobenius 核は $\{a_{1,\beta}\}$ である（問 10.3 より $LF(q)$ は強3重可移である).

定 理 11.11 （1） GをΩ上の Frobenius 群, $H=G_i$ $(i\in\Omega)$ とする. このとき任意の $x\in G-H$ に対して $H\cap H^x=1$ である.

（2） Gを一般の群, Hをつぎの性質をもつGの部分群とする.

$1\lneqq H\lneqq G$ で任意の $x\in G-H$ に対して $H\cap H^x=1$ である.

このときGの部分群 H による置換表現は，忠実な表現で，$(G, G/H)$ は Frobenius 群である．

［証 明］（1） 任意の $x \in G-H$ に対して $i^x \neq i$ であるから，$H \cap H^x = G_i \cap G_{i^x} = G_{i\,i^x} = 1$ である．

（2） 置換表現 $f: G \to (G, G/H)$ において定理 6.5 より，$\ker f = \bigcap_{x \in G} H^x$ である．ここで仮定より $x \in G-H$ に対して，$H \cap H^x = 1$ であるから $\ker f = 1$ となり，f は忠実な表現である．

$G = Hx_1 + Hx_2 + \cdots + Hx_n$，$Hx_1 = H$ とし $\Omega = \{Hx_1, Hx_2, \cdots, Hx_n\}$ とおく．

（i） 定理 6.5 より G^f はΩ上可移である．

（ii） $x(\neq 1) \in H$ に対して，f は忠実だから $x^f \neq 1$ で，$x^f \in (G^f)_H$ である．したがって $(G^f)_H \neq 1$ である．

（iii） 任意の $i(\neq 1) \in \{2, 3, \cdots, n\}$ に対して $x^f \in (G^f)_{H\,Hx_i}$ をとると，$Hx = H$，$Hx_i = Hx_ix$ である．したがって $x \in H$ であり，$x_i^{-1}Hx_i = x_i^{-1}Hx_ix, x \in H^{x_i}$ となり $x \in H \cap H^{x_i}$ である．このとき $x_i \notin H$ だから仮定より $H \cap H^{x_i} = 1$ となり $x = 1$ すなわち $(G^f)_{H\,Hx_i} = 1$ である．

以上より $(G, G/H)$ は Frobenius 群である．□

つぎの定理の証明には群論における多くの性質を用いなくてはならないので，ここで証明することはできないが，置換群論における重要な定理である．

定 理 11.12 (Frobenius, Thompson) Frobenius 群において，Frobenius 核はべき零な正規部分群である．

GをΩ上の置換群とする．Ω上のG-軌道の長さがすべて等しいとき，GはΩ上 $\frac{1}{2}$ **重 可 移** であるという．ここで $G = 1$ は除くが，$|\Omega| = 1$ のときは含めることとする．またGがΩ上 t 重可移で，$G_{1\,2\,\cdots\,t}$ が $\Omega - \{1, 2, \cdots, t\}$ 上$\frac{1}{2}$重可移のとき，GをΩ上 $t + \frac{1}{2}$ $\left(\text{または}\frac{2t+1}{2}\right)$ **重 可 移** であるという．

注 11.13（1） 可移群は$\frac{1}{2}$重可移である．

（2） 可移群の正規部分群（$\neq 1$）は$\frac{1}{2}$重可移である．

（3） 半正則置換群（$\neq 1$）は$\frac{1}{2}$重可移である．

［証 明］（1）は定義より明らかである．（2）は注 5.2 より（3）は定理 11.1 (1) より成り立つ．□

定 理 11.14 $\frac{3}{2}$重可移群は，原始置換群であるか，Frobenius 群である.

［証 明］ GをΩ上の$\frac{3}{2}$重可移群とし，非原始的とする．したがって $\{\Delta_1, \Delta_2, \cdots, \Delta_r\}$ をGの非原始系，$1<|\Delta_i| = m<|\Omega|$, $\Delta_i = \{i_1, i_2, \cdots, i_m\}$ $(i = 1, 2, \cdots, r)$ とし，特に $1_1 = 1$ とする．また $H = G_1$ の軌道を $\{1\}, \Gamma_1, \Gamma_2, \cdots, \Gamma_s$ とする．仮定より $|\Gamma_i| = l > 1$ $(i = 1, 2, \cdots, s)$ で，$H \neq 1$ である．このとき

$$|\Omega| = \sum_{i=1}^{r} |\Delta_i| = rm = 1 + \sum_{i=1}^{s} |\Gamma_i| = 1 + sl$$

となり，$rm = 1 + sl$ より $(m, l) = 1$ である.

Δ_1 と異なる任意の非原始ブロック Δ_i に対して，$\Delta_i{}^H$ はいくつかの非原始ブロックの和集合であるから，$|\Delta_i{}^H|$ はmの倍数である．また $\Delta_i{}^H$ はいくつかの H-軌道の和集合で文字 1 を含まないから，$|\Delta_i{}^H|$ は l の倍数でもある．ここで $(m, l) = 1$ より，$|\Delta_i{}^H|$ は ml の倍数である.

一方 $\Delta_i{}^H = \bigcup_{j=1}^{m} i_j{}^H$, $|i_j{}^H| = l$ より $|\Delta_i{}^H| \leqq ml$ であるから，$|\Delta_i{}^H| = ml$ である．したがって $\Delta_i{}^H = \bigcup_{j=1}^{m} i_j{}^H$ はm個のH-軌道 $i_1{}^H, i_2{}^H, \cdots, i_m{}^H$ の和集合で，Δ_i の m 個の文字 $i_1, i_2, \cdots, i_m$ はすべて異なる H-軌道に属する．このことより，H の元でΔ_i を集合として固定する元は Δ_i の各文字を固定する.

したがって非原始ブロック Δ_i $(\neq \Delta_1)$ の文字 i_j に対して任意の $x \in H_{i_j}$ をとると，$i_j \in \Delta_i \cap \Delta_i{}^x$ より $\Delta_i = \Delta_i{}^x$ となり，上に述べたことより $x \in H_{\Delta_i}$ となる．ここで xは H_{i_j} の任意の元であるから $H_{i_j} \leqq H_{\Delta_i}$ である.

一方 $H_{i_j} = G_{1\,i_j} = G_{i_j 1}$ であるから，上の証明のΔ_iとΔ_1をとりかえることにより

$$H_{i_j} = (G_{i_j})_1 \leqq (G_{i_j})_{\Delta_1} \leqq G_{\Delta_1} = H_{\Delta_1}$$

をうる．したがって任意の $1_{j'} \in \Delta_1 - \{1\}$に対して

$$H_{i_j} \leqq H_{\Delta_1} \leqq H_{1_{j'}}$$

となる．ここでHは $\Omega - \{1\}$上$\frac{1}{2}$重可移であるから，$|H_{i_j}| = |H_{1_{j'}}|$ となり $H_{i_j} = H_{1_{j'}}$ である.

以上において i_j は $\Omega - \Delta_1$ の任意の文字であり，$1_{j'}$ は $\Delta_1 - \{1\}$ の任意の文字であるから，$\Omega - \{1\}$ の任意の文字 i に対して H_i は $\Omega - \{1\}$ のすべての点を固定し，$H_i = 1$ となる．したがってG_1は $\Omega - \{1\}$ 上半正則で，Gは Frobenius 群である．□

問 11.1 $V = V(n, q)$ において，$A(n, q) = \{a; v \mapsto v^\sigma + u | \sigma \in GL(V),\ v, u \in V\}$ とおくとき，$A(n, q)$ はV上2重可移群で，$T = \{t; v \mapsto v + u | v, u \in V\}$ は $A(n, q)$ の正則可換正規部分群であることを示せ.

問 11.2 Gを素数p次の可移置換群，PをGの p-シロー部分群とする．いま $N_G(P) \gneqq P$ であれば，$N_G(P)$ はPを Frobenius 核とする Frobenius 群であることを示せ．

問 11.3 群 $G=\{a_1=1, a_2, \cdots, a_n\}$ に対して，G上の置換 $\varphi(a, b)$ を $\varphi(a, b)=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a^{-1}a_1b & a^{-1}a_2b & \cdots & a^{-1}a_nb \end{pmatrix}$ により定義すると，$\bar{G}=\{\varphi(a,b) \mid a, b \in G\}$ はG上の可移置換群で

(1) Gの中心を $Z(G)$ とすると，$|\bar{G}|=|G|^2/|Z(G)|$ で

(2) $\bar{G}$ の階数はGの共役類の個数に等しい

ことを示せ．

§ 12. 正規部分群

定理 12.1 GをΩ上の可移群，NをGの正則正規部分群とし，$\Omega^*=N-\{1\}$ とおく．このとき $G_1{}^*=\left\{x^*=\begin{pmatrix} a \\ a^x \end{pmatrix} \middle| \, x \in G_1, a \in \Omega^* \right\}$ (ただし $a^x=x^{-1}ax$) は Ω^* 上の置換群で $(G_1, \Omega-\{1\}) \cong (G_1{}^*, \Omega^*)$ である．

［証 明］ NはGの正規部分群であるから，系6.6の証明で示したように，$G_1{}^*$ は G_1 の Ω^* 上の置換表現 $f: x \mapsto x^*=\begin{pmatrix} a \\ a^x \end{pmatrix}$ によりえられた Ω^* 上の置換群である．$x \in \ker f$ とすると任意の $a \in \Omega^*$ に対して $a^x=a$ だから，$C_N(x)=N$である．ここでxはΩ上の置換として1を固定し，NはΩ上正則だから定理 11.5 より $x=1$ となり，fは同型写像である．

NはΩ上正則だから，注 11.4 より $\Omega^*=\{a_2, a_3, \cdots, a_n\}$，$1^{a_i}=i$ $(i=2,3,\cdots,n)$，$\Omega-\{1\}=\{1^{a_2}, 1^{a_3}, \cdots, 1^{a_n}\}$ とすることができる．したがって写像 $\varphi: \Omega-\{1\} \rightarrow \Omega^*$ を $i \mapsto a_i$ により定義すると，φは全単射である．

任意の $i \in \Omega-\{1\}$，任意の $x \in G_1$ に対して，

$$(i^x)^\varphi=(1^{a_i x})^\varphi=(1^{x^{-1}a_i x})^\varphi=a_i{}^x,$$

$$(i^\varphi)^{x^f}=(a_i)^{x^f}=a_i{}^x$$

であるから，$(i^x)^\varphi=(i^\varphi)^{x^f}$ となり $(G_1, \Omega-\{1\}) \cong (G_1{}^*, \Omega^*)$ である．□

定理 12.2 GをΩ上のt重可移群，NをGの正則正規部分群とする．

(1) $t=2$ のとき，Nは位数 p^m (pは素数) の基本可換群である．

(2) $t=3$ のとき，Nの位数は 2^m か，$G=S_3$ でNの位数は3である．

(3) $t=4$ のとき，$G=S_4$ でNは4元群である．

［証明］ 定理 12.1 で定義した $(G_1,\ \Omega-\{1\})$ と同値な置換群である $(G_1{}^*,\ \Omega^*)$ を用いる．

（1） $t=2$ のとき G_1 は $\Omega-\{1\}$ 上可移である．したがって $G_1{}^*$ は $\Omega^*=N-\{1\}$ 上可移である．いま位数が素数 p である $a\in N$ をとる．任意の $b\in N-\{1\}$ に対して，$G_1{}^*$ は Ω^* 上可移であるから，$b=a^x$ となる $x\in G$ が存在する．したがって $N-\{1\}$ の元はすべて位数が p となり，N は p－群である．このとき定理 1;2.3 より N の中心 $Z(N)\neq 1$ であり，特に $a\in Z(N)-\{1\}$ をとることにより，$N-\{1\}$ の元は a とすべて共役になり $Z(N)$ に属す．すなわち N は基本可換群である．

（2） $t=3$ とする．任意の $a\in N-\{1\}$ に対して $\{a,a^{-1}\}$ は $G_1{}^*$ の Ω^* 上の非原始ブロックである．一方 G_1 は $\Omega-\{1\}$ 上 2 重可移だから，$G_1{}^*$ も Ω^* 上 2 重可移になり系 7.7 より $G_1{}^*$ は原始的である．したがって $\{a,a^{-1}\}$ は $G_1{}^*$ の自明な非原始ブロックとなり，$\{a,a^{-1}\}=\{a\}$ か Ω^* となる．

$\{a,a^{-1}\}=\{a\}$ のとき，$a=a^{-1}, a^2=1$ となり N は 2－群である．$\{a,a^{-1}\}=\Omega^*$ のとき，$|N|=3$ となり $G=S_3$ である．

（3） $t=4$ とする．（2）より $|\Omega|=|N|=2^m, m\geqq 2$ である．H^* を $G_1{}^*$ における $a\in\Omega^*$ の安定化群とすると，H^* は $\Omega-\{a\}$ 上 2 重可移したがって原始的である．

いま $b\in\Omega^*-\{a\}$ に対して $\{b,ab\}$ を作り，$\{b,ab\}\cap\{b,ab\}^x\neq\phi$ である元 $x^*\in H^*$ をとる．このとき $(ab)^x=ab^x$ であるから，$b^x=b\Leftrightarrow(ab)^x=ab^x=ab$，$b^x=ab\Leftrightarrow(ab)^x=ab^x=b$ となり，$\{b,ab\}^x=\{b,ab\}$ である．

したがって $\{b,ab\}$ は H^* の非原始ブロックとなり，H^* は原始的であるから，$\{b,ab\}$ は自明な非原始ブロックとなる．このとき $b\neq ab$ であるから $\{b,ab\}=\Omega^*-\{a\}$ となり，$|N|=4$ で N は 4 元群したがって $G=S_4$ である．□

定理 12.3 G は Ω 上の原始置換群で，正則である正規部分群をもたないとする．このとき G_i が単純群であれば G も単純群である．

［証明］ N を G の正規部分群 $(\neq 1)$ とする．系 7.9 より N は Ω 上可移で，仮定より $N_i\neq 1$ である．さらに $N_i=G_i\cap N\trianglelefteq G_i$ で G_i は単純であるから，$N_i=G_i$ である．したがって $|N|=|\Omega|\cdot|N_i|=|\Omega|\cdot|G_i|=|G|$ となり，$G=N$ すなわち G は単純群である．□

定理 12.4 G を Ω 上の原始置換群，N を G の正規部分群 $(\neq 1)$ とする．

（1） N が正則であれば，N は G の極小正規部分群である．

（2） N が可解な極小正規部分群であれば，N は正則な基本可換群で，G の

極小正規部分群はNのみである.

（3） N が可換群であれば，N はGの極小正規部分群になり（2）をみたす.

［証明］（1） MをNに含まれるGの正規部分群（$\neq 1$）とする．系 7.9 よりMはΩ上可移で，したがって $|M| \geqq |\Omega|$ である．一方Nは正則であるから $|\Omega| = |N|$ である．これより $M = N$ となり，NはGの極小正規部分群である.

（2） Nの交換子群 $[N, N]$ をとると，Nは可解だから $N \gneqq [N, N]$ である．さらに $N \trianglelefteq G$ であるから $[N, N] \trianglelefteq G$ となり，NはGの極小正規部分群であるから $[N, N] = 1$ となり，Nは可換群である.

さらにGは原始的だからNは可移で，系 11.10 よりNは正則である．いまpをNの位数を約する素数とし，$N^{(p)} = \{x \in N \mid x^p = 1\}$ とおく．N は可換群でGの正規部分群だから，$N^{(p)}$ もGの正規部分群である．さらにNは $x^p = 1$ となる元 $x (\neq 1)$ をもつから $1 \lneqq N^{(p)}$ となり，Nの極小性より $N^{(p)} = N$ である．したがってNの元（$\neq 1$）はすべて位数pとなり，Nは基本可換群である.

Nと異なるGの極小正規部分群Mが存在するとする．このとき$M \cap N \trianglelefteq G$ であるからNの極小性より $M \cap N = 1$ である．したがって定理 1; 4.1 より $[M, N] = 1$ となり $M \leqq C_G(N)$ である．しかしNは正則な可換群であるから，系 11.8 より $C_G(N) = N$ で $M \leqq N$ となり，Mについての仮定に反する．したがってGの極小正規部分群はNのみである.

（3） Nを可換な正規部分群とすると，Nは可移で系 11.10 より正則である．したがって（1）よりNはGの極小正規部分群になり，Nは（2）をみたす．□

定理 12.5 (Burnside) GをΩ上の 2 重可移群，NをGの極小正規部分群とする.

（1） Nが正則であれば，Nは基本可換群でGの極小正規部分群はNのみである.

（2） Nが正則でないならば，Nは原始的な単純群である.

［証明］（1） Nを正則とすると，定理 12.2（1）よりNは基本可換群で，さらに定理 12.4（2）よりGの極小正規部分群はNのみである.

（2） N は正則でないとする．Gは 2 重可移だから，N は可移で，$1 \lneqq N_1 \trianglelefteq G_1$ であり，注 11.13（2）より N_1 は $\Omega - \{1\}$ 上 $\frac{1}{2}$ 重可移である．したがってNはΩ上 $\frac{3}{2}$ 重可移となり，定理 11.14 よりNは原始置換群であるか Frobenius 群である.

Nが Frobenius 群であれば，Frobenius 核は定理11.12よりNの特性部分群になり，

したがってGの正規部分群になりNの極小性に反する．したがってNは原始置換群である．

Nは単純でないとし，MをNの極小正規部分群とする．仮定よりMはGの正規部分群でないから，$M^a \neq M$ となる $a \in G$ が存在する．このとき $M \lhd N \trianglelefteq G$ だから $M^a \lhd N^a = N$ である．またMはNの極小正規部分群だから，$M \cap M^a = 1$ となり定理 1;4.1 より $[M \cap M^a] = 1$ すなわち $M^a \leqq C_G(M)$ である．

Nは原始的であるから，M, M^a は共にΩ上可移である．したがって $M^a \leqq C_G(M)$ より $C_G(M)$ も Ω 上可移になり定理 11.9 よりMは正則であり，M^a も正則になる．さらに定理 11.6 より $M^a = C_G(M)$ である．

$M^x \neq M$ である任意の $x \in G$ に対して，M^a と同様にして $M^x = C_G(M)$ である．したがって $M^x = M^a$ となり，$MM^a \trianglelefteq G$ である．ここでNはGの極小正規部分群であるから，$N = MM^a$ となる．

Mは正則であるから，$|M| = |\Omega| = n$ したがって $|N| = n^2, |N_1| = n$ となる．NはΩ上 3/2 重可移だから，$\Omega - \{1\}$ 上の N_1-軌道の長さはすべて等しく，いまその長さを l とすると $n-1$ の約数である．一方 $|N_1| = n$ であるから l は n の約数でもあり，$(n, n-1) = 1$ より $l = 1$ となる．よって $N_1 = 1$ になりNが正則でないことに反する．

以上よりNは単純群である．□

定 理 12.6 (Wagner)　Gを奇数次 ($\geqq 3$) の 3 重可移群とすると，Gの正規部分群 ($\neq 1$) も 3 重可移である．

［証 明］ GをΩ上の 3 重可移群，NをG の正規部分群 ($\neq 1$) とする．系 7.9 よりNはΩ上可移である．Nが正則であれば，定理 12.2 (2) より $|\Omega|$ は 2 のべきかまたは 3 となり仮定に反する．したがって $1 \lneqq N_1 \trianglelefteq G_1$ で G_1 は $\Omega - \{1\}$ 上 2 重可移であるから，N_1 も $\Omega - \{1\}$ 上可移となり，NはΩ上 2 重可移である．なお以下の証明でGの元を巡回置換の積で示したときはつねに巡回表示とする．

任意の $i, j, k (\neq) \in \Omega$ をとる．Nは 2 重可移だから，位数 2 の元 $a = (i\ j) \cdots$ をもつ．さらに $|\Omega|$ は奇数だから a は固定点をもち $a = (i\ j)(k') \cdots$ である．このときGは 3 重可移だから $x = \begin{pmatrix} i & j & k' & \cdots \\ i & j & k & \cdots \end{pmatrix} \in G$ が存在し，$a^x = (i\ j)(k) \cdots$ となり，$N \trianglelefteq G$ より $a^x \in N$ である．すなわち異なる任意の 3 点 i, j, k に対して，Nは $(i\ j)(k) \cdots$ なる位数 2 の元をもつ．

Nにおける $\{1, 2\}$ の集合としての安定化群 $N_{\{1,2\}}$ と点ごとの安定化群 $N_{1\,2}$ をとると，$N_{\{1,2\}} \rhd N_{1\,2}$ である．Γを $\Omega - \{1, 2\}$ 上の $N_{\{1,2\}}$-軌道とする．いま $|\Gamma| > 1$ とする．

任意の $i, j(\neq)\in\Gamma$ に対して，$i^x=j$ なる $x\in N_{(1,2)}$ が存在する．$x\notin N_{1\,2}$ とすると $x=(1\ 2)(i\ j\ \cdots)\cdots$ である．一方上で示したことより $y=(1\,2)(j)\cdots\in N$ が存在するから，$xy=(1)(2)(i\ j\ \cdots)\cdots\in N_{1\,2}$ となり $i^{xy}=j$ である．ここで i, j は $N_{(1,2)}$-軌道 Γ の任意の2点であるから，Γ は $N_{1\,2}$-軌道でもある．$|\Gamma|=1$ のときはもちろん Γ は $N_{1\,2}$-軌道である．以上より $\Omega-\{1,2\}$ 上の $N_{(1,2)}$-軌道と $N_{1\,2}$-軌道は一致する．

$G_{1\,2}$ は $\Omega-\{1,2\}$ 上可移で，$G_{1\,2}\geqq N_{1\,2}$ だから注5.2より $\Omega-\{1,2\}$ 上の $N_{1\,2}$-軌道の長さは等しい．さらに $|\Omega-\{1,2\}|$ は奇数だから，$\Omega-\{1,2\}$ 上の $N_{1\,2}$-軌道の長さは奇数である．

いま N_{12} は $\Omega-\{1,2\}$ 上可移でないとし，$\Omega-\{1,2\}$ 上の N_{12}-軌道の個数を r (>1) とする．P を $N_{(1,2)}$ の 2-シロー部分群とすると，$|N_{(1,2)}|$ は偶数だから $P\neq 1$ である．このとき $|N_{(1,2)}:N_{1\,2}|=2$ より $N_{1\,2}$ の 2-シロー部分群の位数は $|P|/2$ である．$\Omega-\{1,2\}$ 上の $N_{(1,2)}$-軌道と $N_{1\,2}$-軌道は一致するから，その長さはすべて奇数であり，したがって各 $N_{(1,2)}$-軌道に P は少なくとも1つ固定点をもつ．すなわち $|F(P)|\geqq r\gneqq 1$ である．いま $i_1, i_2(\neq)\in F(P)$ をとると，$N_{i_1 i_2}\geqq P$ である．一方 N は2重可移だから $|N_{1\,2}|=|N_{i_1\,i_2}|$ である．したがって $N_{i_1\,i_2}$ の 2-シロー部分群の位数は $|P|/2$ になり，$N_{i_1\,i_2}\geqq P$ に反する．

以上より $N_{1\,2}$ は $\Omega-\{1,2\}$ 上可移になり，N は Ω 上3重可移である．□

$|\Omega|$ が偶数のとき，3重可移群の正規部分群は3重可移とは限らない．

例 1.　$\Omega=\{1,2,3,4\}$ 上の対称群 S_4 は Ω 上4重可移であるが，交代群 A_4，4元群 $\langle(1\ 2)(3\ 4),(1\ 3)(2\ 4)\rangle$ は共に S_4 の正規部分群であるが，Ω 上3重可移ではない．

例 2.　$PG(1,q)$ 上の置換群 $PGL(2,q)$ は定理10.6より3重可移で，q を奇数にとると $|PG(1,q)|=1+q$ は偶数になる．このとき $PSL(2,q)$ は $PGL(2,q)$ の正規部分群で，$|PSL(2,q)|=(q+1)\cdot q\cdot(q-1)/2$ である．$PSL(2,q)$ は定理10.5より $PG(1,q)$ 上2重可移群であるが，2点の安定化群は位数が $(q-1)/2$ であるから，$q-1$ 個の文字の上で可移になりえない．すなわち $PSL(2,q)$ は3重可移ではない．

問 12.1　G を可解群とすると，G の極大部分群の G における指数は素数べきであることを示せ．

問 12.2　G を $\Omega=\{1,2,\cdots,n\}$ 上の位数 $n(n-1)$ の Frobenius 群とする．このとき Frobenius 核 $N=\{a\in G\mid F(a)=\phi\}\cup\{1\}$ は，G の正則正規部分群で基本可換群であることを，定理11.12を用いずに示せ．

問 12.3　Gをn次の2重可移群とする．Gが非原始正規部分群をもてば，nは素数べきであることを示せ．

問 12.4　次数6の原始置換群を求めよ．

§13. 対称群，交代群の基本関係と自己同型群

$\{a_1, a_2, \cdots, a_n\}$ を群Gの生成系とし，$a_1, a_2, \cdots, a_n$ の間のいくつかの関係式の集合　$R = \{f_i(a_1, a_2, \cdots, a_n) = a_{i_1}{}^{r_1} a_{i_2}{}^{r_2} \cdots a_{i_k}{}^{r_k} = 1 \mid i \in I\}$　が与えられているとする．いま $\{a_1', a_2', \cdots, a_n'\}$ を生成系とする群 G' が，Gと同じ関係式をもつ．すなわちRのすべての元 $f_i(a_1, a_2, \cdots, a_n) = 1$ に対して $f_i(a_1', a_2', \cdots, a_n') = 1$ とする．このときGからG'の上への準同型φで，$a_i{}^\varphi = a_i'(i = 1, 2, \cdots, n)$ となるものが存在するならば，RをGの生成元の間の **基本関係** という．

一般に，任意に与えられた関係式を基本関係とする群が存在することが，自由群を用いて証明される．

補 題 13.1　n次の対称群S_nは $n-1$ 個の互換 $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ で生成される．

［**証 明**］ 任意の互換 $(i\ i+k)$ $(k \geqq 1)$ は　$a = (i+1\ i+2)(i+2\ i+3) \cdots (i+k-1\ i+k)$　とおくと $a^{-1}(i\ i+1)a$ に等しい．したがって　$S = \langle (1\ 2), (2\ 3), \cdots, (n\ n-1) \rangle$　である．□

ここで $a_i = (i\ i+1)$ $(i = 1, 2, \cdots, n)$ とおくと，$a_i{}^2 = (a_i a_{i+1})^3 = (a_i a_j)^2 = 1$ $(|i-j| > 1)$ である．これが S_n の生成元 $a_1, a_2, \cdots, a_n$ の間の基本関係になることがつぎのようにして示される．

定 理 13.2　群 $G = \langle a_1, a_2, \cdots, a_{n-1} \rangle$ において基本関係を

$$a_i{}^2 = 1 \qquad (i = 1, 2, \cdots, n-1),$$
$$(a_i\ a_{i+1})^3 = 1 \qquad (i = 1, 2, \cdots, n-2),$$
$$(a_i\ a_j)^2 = 1 \qquad (|i-j| > 1,\ i, j = 1, 2, \cdots, n-1)$$

とすると，Gは S_n に同型である．

［**証 明**］ S_n において $a_i' = (i\ i+1)$ $(i = 1, 2, \cdots, n-1)$ とおけば，$a_1', a_2', \cdots, a_n'$ は上の関係式をみたすから，基本関係の定義よりS_nはGの準同型像である．したがって $|G| \leqq |S_n|$ を示せばGと S_n は同型になる．いまこれをnに関する帰納法で証明する．

$n = 2$のとき $|G| = |S_n| = 2$ となり成立する．

いま $H=\langle a_1, a_2, \cdots, a_{n-2}\rangle \cong S_{n-1}$ と仮定する．このとき $|G{:}H| \leqq n$ を示せばよい．したがってGのHによる左剰余類

$$H_1 = Ha_{n-1}a_{n-2}\cdots a_1,\quad H_2 = Ha_{n-1}a_{n-2}\cdots a_2,\quad \cdots,\quad H_{n-1} = Ha_{n-1},\quad H_n = H$$

を作るとき，任意の $x \in G$ に対して $Hx \in \{H_1, H_2, \cdots, H_n\}$ を示せば $G = \bigcup_{x\in G} Hx = H_1 \cup H_2 \cup \cdots \cup H_n$ となり，$|G:H| \leqq n$ となる．ここで任意の $x \in G$ はGの生成元 $a_1, a_2, \cdots, a_n$ の有限個の積で書けるから，その個数に関する帰納法で，$Hx \in \{H_1, H_2, \cdots, H_n\}$ を示す．

$x = a_j\ (j = 1, 2, \cdots, n-1)$ とする．$j = 1, 2, \cdots, n-2$ のとき $Hx = H = H_n$ である．$x = a_{n-1}$ のとき $Hx = H_{n-1}$ である．

いま $x = a_{i_1}a_{i_2}\cdots a_{i_j}$ とし $Ha_{i_1}a_{i_2}\cdots a_{i_{j-1}}$ はある H_i に等しいと仮定する．したがって任意の a_j について $H_i a_j \in \{H_1, H_2, \cdots, H_n\}$ を示せばよい．

$(a_k a_{k+1})^3 = 1, a_k{}^2 = 1$ より $a_{k+1}a_k a_{k+1} = a_k a_{k+1} a_k$ である．また $|k-k'| > 1$ のとき $(a_k a_{k'})^2 = 1, a_k{}^2 = a_{k'}{}^2 = 1$ より $a_k a_{k'} = a_{k'} a_k$ である．これらを用いてつぎのようになる．

$j < i-1$ のとき　$H_i a_j = Ha_{n-1}\cdots a_i \cdot a_j = Ha_j \cdot a_{n-1} \cdots a_i = Ha_{n-1}\cdots a_i = H_i$ である．

$j = i-1$ のとき　$H_i a_{i-1} = Ha_{n-1}\cdots a_i \cdot a_{i-1} = H_{i-1}$ である．

$j = i$ のとき　$H_i a_i = Ha_{n-1}\cdots a_i \cdot a_i = Ha_{n-1}\cdots a_{i+1} = H_{i+1}$ である．

$j > i$ のとき　$H_i a_j = Ha_{n-1}\cdots a_i \cdot a_j = Ha_{n-1}\cdots a_{j+1}a_j a_{j-1}\cdot a_j \cdot a_{j-2}\cdots a_i$
$= Ha_{n-1}\cdots a_{j+1}\cdot a_{j-1}a_j a_{j-1}\cdot a_{j-2}\cdots a_i = Ha_{j-1}\cdot a_{n-1}\cdots a_i = Ha_{n-1}\cdots a_i$
$= H_i$ である．

以上より $H_i a_j \in \{H_1, H_2, \cdots, H_n\}$ となり，したがって $|G:H| \leqq n$ が成り立ち定理は証明された．□

補題 13.3 n 次の交代群 $A_n (n \geqq 3)$ は $n-2$ 個の元 $a_1 = (1\ 2\ 3)$, $a_2 = (1\ 2)(3\ 4)$, $\cdots$, $a_{n-2} = (1\ 2)(n-1\ n)$ で生成される．

［**証明**］ n に関する帰納法で証明する．

$n=3$ のとき $A_3 = \langle a_1 \rangle$ である．

いま $A_{n-1} = \langle a_1, a_2, \cdots, a_{n-3}\rangle$ と仮定する．$G = \langle A_{n-1}, a_{n-2}\rangle$ とおくと，A_{n-1} は $\{1, 2, \cdots, n-1\}$ 上可移で，$a_{n-2} = (1\ 2)(n-1\ n)$ より G は $\{1, 2, \cdots, n\}$ 上可移となる．したがって G における文字 n の安定化群を H とすると，$H \geqq A_{n-1}$, $|G{:}H| = n$ となり，$|A_{n-1}| = (n-1)!/2$ より $|G| \geqq n!/2$ である．一方 G の生成元は偶置換のみで

あるから $G \leqq A_n$ で，したがって $G = A_n$ である．□

ここで $a_1{}^3 = a_i{}^2 = 1$ $(i = 2, 3, \cdots, n-2)$, $(a_ia_{i+1})^3 = (a_ia_j)^2 = 1$ $(|i-j| > 1,\ i, j = 1, 2, \cdots, n-2)$ である．これが A_n の生成元 $a_1, a_2, \cdots, a_{n-2}$ の間の基本関係になることがつぎのようにして示される．

定理 13.4 群 $G = \langle a_1, a_2, \cdots, a_{n-2}\rangle$ において，基本関係を

$$a_1{}^3 = a_i{}^2 = 1 \qquad (i = 2, 3, \cdots, n-2),$$
$$(a_ia_{i+1})^3 = 1 \qquad (i = 1, 2, \cdots, n-3),$$
$$(a_ia_j)^2 = 1 \qquad (|i-j| > 1, i, j = 1, 2, \cdots, n-2)$$

とすると，Gは A_n に同型である．

［**証 明**］ 定理 13.2 と同様にして証明される．

A_n において $a_1' = (1\ 2\ 3)$, $a_i' = (1\ 2)(i+1\ \ i+2)$ $(i = 2, 3, \cdots, n-2)$ とおけば上の関係式をみたすから，基本関係の定義より A_n はGの準同型像である．したがって $|G| \leqq |A_n|$ を示せばGと A_n は同型になる．いまこれを n に関する帰納法で証明する．

$n = 3$ のとき $|G| = |A_3| = 3$ となり成立する．

いま $H = \langle a_1, a_2, \cdots, a_{n-3}\rangle \cong A_{n-1}$ と仮定する．このとき $|G : H| \leqq n$ を示せばよい．したがってGのHによる左剰余類

$$H_1 = Ha_{n-2}a_{n-3}\cdots a_1,\quad H_2 = a_{n-2}a_{n-3}\cdots a_2\cdot a_1{}^{-1},\quad H_3 = Ha_{n-2}a_{n-3}\cdots a_2,$$
$$H_{n-1} = Ha_{n-2},\quad H_n = H$$

を作るとき，任意の $x \in G$ に対して $Hx \in \{H_1, H_2, \cdots, H_n\}$ を示せば，$G = \bigcup_{x\in G} Hx = H_1 \cup H_2 \cup \cdots \cup H_n$ となり，$|G:H| \leqq n$ となる．ここで任意の $x \in G$ はGの生成元 $a_1, a_2, \cdots, a_{n-2}$ の有限個の積で書けるから，その個数に関する帰納法で，$Hx \in \{H_1, H_2, \cdots, H_n\}$ を示す．

$x = a_j$, $j = 1, 2, \cdots, n-2$ とする．$j = 1, 2, \cdots, n-3$ であれば，$Hx = H = H_n$ である．$x = a_{n-2}$ のときは $Hx = H_{n-1}$ である．

いま $x = a_{i_1}a_{i_2}\cdots a_{i_j}$ とし $Ha_{i_1}a_{i_2}\cdots a_{i_{j-1}}$ はある H_i に等しいと仮定する．したがって任意の a_j について $H_ia_j \in \{H_1, H_2, \cdots, H_n\}$ を示せばよい．

$a_1{}^3 = a_i{}^2 = 1$ $(i = 2, 3, \cdots, n-2)$ を用いて，$(a_1a_2)^3 = 1$ より $a_2a_1a_2 = a_1{}^{-1}a_2a_1{}^{-1}$, $a_2a_1{}^{-1}a_2 = a_1a_2a_1$ である．さらに $(a_1a_i)^2 = 1$ $(i = 3, 4, \cdots, n-2)$ より $a_ia_1 = a_1{}^{-1}a_i$. $(a_ia_{i+1})^3 = 1$ $(i = 2, 3, \cdots, n-2)$ より $a_ia_{i+1}a_i = a_{i+1}a_ia_{i+1}$. $(a_ia_j)^2 = 1$

$(|i-j|>1,\ i,j=2,3,\cdots,n-2)$ より $a_ia_j=a_ja_i$ である．これらを用いてつぎのようになることはみやすい．

$H_1a_1=H_2,\ H_2a_1=H_3,\ H_3a_1=H_1$ で $i\geqq 4$ に対して $H_ia_1=H_i$ である．

$j\geqq 2$ のとき，$H_1a_j=H_2,\ H_2a_j=H_1,\ H_{j+1}a_j=H_{j+2},\ H_{j+2}a_j=H_{j+1}$ で，$i\neq 1,2,j+1,j+2$ のとき $H_ia_j=H_i$ である．

以上より $H_ia_j\in\{H_1,H_2,\cdots,H_n\}$ となり，したがって $|G:H|\geqq n$ が成り立ち定理は証明された．□

定理 13.5 （1） $n\neq 6$ のとき対称群 S_n の任意の自己同型は内部自己同型である．したがって $\mathrm{Aut}\,S_n=\mathrm{Inn}\,S_n\ (\cong S_n, n\neq 2)$ である．

（2） 対称群 S_6 においては，$\mathrm{Inn}\,S_6\cong S_6$ で，$|\mathrm{Aut}\,S_6:\mathrm{Inn}\,S_6|=2$ である．

［証 明］ S_n の互換全体は定理 3.2 より S_n の 1 つの共役類を作る．いまこの共役類を C とおく．

$f\in\mathrm{Aut}\,S_n$ に対して C^f はまた S_n の共役類である．いま $C^f=C$ とする．$(1\ 2)$, $(1\ 3),\cdots,(1\ n)$ は S_n を生成する C の元であるから，これらの f による像を考える．$(1\ 2)^f=(i\ j)$, $(1\ 3)^f=(k\ l)$ とする．ここで S_2 については $\mathrm{Aut}\ S_2=\mathrm{Inn}\,S_2=1$ であるから，定理は成り立つので $n\geqq 3$ とする．このとき

$$((1\ 2)(1\ 3))^f=(1\ 2\ 3)^f=(1\ 2)^f\ (1\ 3)^f=(i\ j)(k\ l)$$

である．したがって $(i\ j)(k\ l)$ は位数 3 の元となり，$\{i,\ j\}$ と $\{k,\ l\}$ は共通な文字を 1 つもつ．すなわち $(1\ 2)^f=(i_1\ i_2)$, $(1\ 3)^f=(i_1\ i_3)$, $i_2\neq i_3$ となる．同様にして $j\geqq 4$ に対して，$(1\ j)^f=(i_1\ i_j)$ または $(i_2\ i_3)$, $i_j\neq i_2,\ i_3$ となる．いま $(1\ j)^f=(i_2\ i_3)$ とすると

$$((1\ 2)(1\ 3)(1\ j))^f=(1\ 2\ 3\ j)^f=(i_1\ i_2)(i_1\ i_3)(i_2\ i_3)=(i_1\ i_3)$$

となり，$(1\ 2\ 3\ j)^f$ の位数は 4 であるから矛盾である．したがって $(1\ j)^f=(i_1\ i_j)$, $i_j\neq i_2,i_3$ である．これより，

$$(1\ 2)^f=(i_1\ i_2),\quad (1\ 3)^f=(i_1\ i_3),\quad \cdots,\quad (1\ n)^f=(i_1\ i_n)$$

となり，$(i_1\ i_2),\ (i_1\ i_3),\ \cdots,\ (i_1\ i_n)$ はすべて異なる互換であるから，$i_1,i_2,\ \cdots,i_n$ はすべて異なる．

一方 S_n に元 $a=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$ が存在し，任意の $j\in\Omega-\{1\}$ に対して $(1\ j)^f=(1\ j)^a$ である．ここで $(1\ 2),(1\ 3),\ \cdots,\ (1\ n)$ は S_n を生成するから自己同型 f と内部自己同型 a は一致する．

つぎに $C^f\neq C$ とし，C^f は位数 2 の元からなるから，巡回表示が $r\,(>1)$ 個の互換

の積である元の作る共役類とする．このとき $x \in C$ に対して $(C_{S_n}(x))^f = C_{S_n}(x^f)$ より，$|C_{S_n}(x)| = |C_{S_n}(x^f)|$ である．さらに系 7.18 より $C_{S_n}(x) \cong S_{n-2} \times \langle x \rangle$ となり，$|C_{S_n}(x)| = (n-2)! \cdot 2$ である．また $C_{S_n}(x^f) \cong S_{n-2r} \times (S_2 \wr S_r)$ より $|C_{S_n}(x^f)| = (n-2r)! \cdot 2^r \cdot r!$ である．したがって

$$(n-2)! \cdot 2 = (n-2r)! \cdot 2^r \cdot r!$$

$$2^{r-1} = (n-2)!/(n-2r)! \cdot r! = \binom{n-2}{n-2r} \cdot (n-2-n+2r)!/r!$$

$$= \binom{n-2}{2r-2} \cdot (2r-2)!/r!$$

である．ここで $r > 1$ より左辺は2のべき（$\neq 1$）であるから，右辺の $(2r-2)!/r!$ も $r > 1$ より整数になり2のべきである．したがって $(2r-2)! = r!$ または $(r+1)!$ すなわち $2r-2 = r$ または $r+1$ となり $r = 2$ または3である．

$r = 2$ のとき上式は $2 = \binom{n-2}{2} = (n-2)(n-3)/2$ となり，これをみたす n は存在しない．

$r = 3$ のとき上式は $2^2 = \binom{n-2}{4} \cdot 4$ となり $n = 6$ である．以上より $n \neq 6$ のとき任意の $f \in \mathrm{Aut}\, S_n$ に対して $C^f = C$ となり $\mathrm{Aut}\, S_n = \mathrm{Inn}\, S_n$ である．

$n = 6$ のとき $r = 3$ であるから，f は $(2,2,2)$ 型の位数2の元よりなる共役類への写像である．このような自己同型は注 6.10 (2) で示した S_5 に同型な6次の群による S_6 の置換表現として存在する．さらに任意の $f, g \in \mathrm{Aut}\, S_6 - \mathrm{Inn}\, S_6$ に対して，$C^f = C^g$ であるから，$C^{fg^{-1}} = (C^f)^{g^{-1}} = (C^g)^{g^{-1}} = C$，$fg^{-1} \in \mathrm{Inn}\, S_6$ である．したがって $|\mathrm{Aut}\, S_6 : \mathrm{Inn}\, S_6| = 2$ である．

また $n \neq 2$ のとき $Z(S_n) = 1$ であるから，定理 1;3.5 より $\mathrm{Inn}\, S_n \cong S_n/Z(S_n) = S_n$ である．□

注 6.10 (2) の証明で示したように $f \in \mathrm{Aut}\, S_6 - \mathrm{Inn}\, S_6$ をたとえばつぎのように定義できる．

$(1\ 2)^f = (1\ 2)(3\ 4)(5\ 6)$,　　$(1\ 3)^f = (1\ 3)(2\ 5)(4\ 6)$,

$(1\ 4)^f = (1\ 4)(2\ 6)(3\ 5)$,　　$(1\ 5)^f = (1\ 5)(2\ 4)(3\ 6)$,

$(1\ 6)^f = (1\ 6)(2\ 3)(4\ 5)$.

定理 13.6 (1) $\mathrm{Aut}\, A_3$ は位数2である．

(2) $n \geqq 4$ のとき $\mathrm{Aut}\, A_n = \mathrm{Aut}\, S_n$ である．

［**証明**］ C を A_n のすべての 3-巡回置換よりなる集合とする．異なる2つの 3-巡回置換の積は，i, j, k, i', j', k' をすべて異なる文字とするとき

$$(i\ j\ k)(i'\ j'\ k'),\qquad (i\ j\ k)(i\ j'\ k')=(i\ j\ k\ j'\ k'),$$
$$(i\ j\ k)(i\ j\ k')=(i\ k')(j\ k),\qquad (i\ j\ k)(i\ k'\ j)=(j\ k\ k'),$$
$$(i\ j\ k)(i\ k\ j)=1$$

の5通りが存在する.

$f\in \mathrm{Aut}\,A_n$ が $C^f=C$ とする. $A_n=\langle(1\ 2\ 3),\ (1\ 2\ 4),\cdots,(1\ 2\ n)\rangle$ で, 各生成元の f による像はつぎのように決まる. $(1\ 2\ 3)^f=(i_1\ i_2\ i_3)$ とする. $(1\ 2\ 3)(1\ 2\ 4)=(1\ 4)(2\ 3)$ だから,

$$((1\ 2\ 3)(1\ 2\ 4))^f=(1\ 2\ 3)^f\ (1\ 2\ 4)^f=(i_1\ i_2\ i_3)\ (1\ 2\ 4)^f$$

も位数が2である. したがって上に示したことより $(1\ 2\ 4)^f=(i_1\ i_2\ i_4)$, $i_3\neq i_4$ となる. 同様にして $j\geqq 5$ に対して, $(1\ 2\ 3)^f=(i_1\ i_2\ i_3)$ より $(1\ 2\ j)^f=(i_1\ i_2\ i_j)$, $(i_2\ i_3\ i_j)$ または $(i_3\ i_1\ i_j)$ である. ここで $(1\ 2\ 4)^f=(i_1\ i_2\ i_4)$ であるから $(1\ 2\ j)^f=(i_1\ i_2\ i_j)$, $i_j\neq i_3,\ i_4$ となる. これより $(1\ 2\ 3)^f=(i_1\ i_2\ i_3)$, $(1\ 2\ 4)^f=(i_1\ i_2\ i_4),\cdots,(1\ 2\ n)^f=(i_1\ i_2\ i_n)$ となり, $i_1,i_2,\cdots,i_n$ はすべて異なる.

一方 S_n に元 $a=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$ が存在し, 任意の $j\in\{3,4,\cdots,n\}$ に対してこの a を用い $(1\ 2\ j)^f=(1\ 2\ j)^a$ である. ここで $(1\ 2\ 3),(1\ 2\ 4),\cdots,(1\ 2\ n)$ は A_n を生成するから f は a による内部自己同型と一致する.

$n=3,\ 4,\ 5$ のとき, A_n の位数3の元は C の元のみであるから, 任意の $f\in \mathrm{Aut}\,A_n$ に対して $C^f=C$ である. これより $\mathrm{Aut}\,A_n$ は S_n の元による A_n の変換と一致する. したがって定理 1;3.5 より $\mathrm{Aut}\,A_3\cong S_3/C_{S_3}(A_3)=S_3/A_3, n=4,5$ のとき

$$\mathrm{Aut}\,A_n\cong S_n/C_{S_n}(A_n)=S_n/1=S_n\cong \mathrm{Aut}\,S_n$$

である.

$n\geqq 6$ とし, x を巡回表示が r 個の 3-巡回置換の積である A_n の位数3の元とする. $r=1$ のとき x と可換な互換が存在する. $r\geqq 2$ とし $x=(i_1\ i_2\ i_3)(j_1\ j_2\ j_3)\cdots$ とすると, $(i_1\ j_1)(i_2\ j_2)(i_3\ j_3)$ は x と可換な奇置換である. したがって r の値に関係なく $|C_{S_n}(x):C_{A_n}(x)|=2$ である. ここで系 7.18 より

$$C_{S_n}(x)\cong S_{n-3r}\times(\langle\bar{x}\rangle\wr S_r),\qquad \langle\bar{x}\rangle=\langle(1\ 2\ 3)\rangle$$

であるから, $|C_{A_n}(x)|=(n-3r)!\cdot 3^r\cdot r!/2$ である.

$n\geqq 6$ であるから, 定理3.8 より C は A_n の共役類となり, C^f も A_n の共役類で位数3の元よりなる. したがって C^f を巡回表示が r 個の 3-巡回置換の積である置換の作る共役類とする. $|C|=|C^f|$ より $x\in C$ に対して $|C_{A_n}(x)|=|C_{A_n}(x^f)|$ となり上で示したことより,

$$(n-3)!\cdot 3/2=(n-3r)!\cdot 3^r\cdot r!/2$$

となり

$$3^{r-1}=(n-3)!/(n-3r)!\cdot r!=\binom{n-3}{n-3r}\cdot(n-3-n+3r)!/r!$$
$$=\binom{n-3}{3r-3}\cdot(3r-3)!/r!$$

となる．いま $r>1$ とすると，左辺は3のべき（$\neq 1$）であるから $(3r-3)!/r!$ も3のべきとなり，$(3r-3)!=r!$ または $(r+1)!$ すなわち $3r-3=r$ または $r+1$ となり，r は整数より $r=2$ となる．このとき $3=\binom{n-3}{3}\cdot 3!/2!$ より $n=6$ である．

以上より $n>6$ のとき $C^f=C$ となり，Aut A_n は S_n の元による A_n の変換全体と一致し，Aut $A_n\cong S_n\cong$ Aut S_n である．

$n=6$ のとき，定理 13.5 (2) と同様にして C^f は (3, 3) 型の作る共役類で，f は Aut S_6 − Inn S_6 の元を A_6 に制限したもので，Aut A_6 = Aut S_6 となる．□

3 Mathieu 群

§1. Mathieu 群の構成

Mathieu 群は，群論において重要な多重可移群である．この節では Witt による Mathieu 群の構成について述べる．

HをΩ上の置換群，Gを$\Omega\cup\{\bar{1}\}, \bar{1}\notin\Omega$上の置換群とし，$G$が$\Omega\cup\{\bar{1}\}$上可移で，$(G_{\bar{1}})^{\Omega}=H$ のときGをHの **可移拡大** (transitive extension) という．

いま $H=\langle(1\ 2)\rangle$ とする．H を $\{1,2\}$ 上の置換群と考えたとき，$\{1,2,3\}$ 上の対称群 S_3 はHの可移拡大である．しかし $\{1,2,3,4\}$ 上の置換群を考えたとき，$G=\langle(1\ 3\ 2\ 4),(1\ 2)\rangle$ はやはりHの可移拡大である．この混乱をさけるために，HがΩ上可移群のときは，Hの可移拡大は$\Omega\cup\{\bar{1}\}, \bar{1}\notin\Omega$で考えることにする．

定理 1.1 $\Omega=\{1,2,\cdots,n\}$とし，Hは文字1を固定し，$\Omega-\{1\}$ 上の2重可移群とする．Ω上の置換 $a=(1\ 2)(3)\cdots$ およびHの元 $b=(1)(2\ 3)\cdots$ が

（1） $a^2\in H$, $(ab)^3\in H$

（2） $(H_2)^a=H_2$

をみたすならば，$G=\langle H, a\rangle$ はHの可移拡大である．したがってGはΩ上3重可移で，$G=H+HaH$ である．

［証明］ $\bar{G}=H\cup HaH$ とおき，$\bar{G}$ が群になることを示す．そのためには定理 1;1.3 より $\bar{G}\bar{G}=\bar{G}$ を示せばよい．

$$\bar{G}\bar{G}=(H\cup HaH)(H\cup HaH)=H\cup HaH\cup HaHaH$$

である．Hは $\Omega-\{1\}$ 上2重可移であるから，$b=(1)(2\ 3)\cdots\in H$ が存在し，系 2;4.8 より $H=H_2+H_2bH_2$ である．したがって

$$HaHaH=Ha(H_2\cup H_2bH_2)aH=HaH_2aH\cup HaH_2bH_2aH$$

である．ここで条件（1）の $a^2\in H$ より $Ha=Ha^{-1}$ であり，$(ab)^3=ababab\in H$ より $H\,aba\,H=Hb^{-1}a^{-1}b^{-1}H=Ha^{-1}H=HaH$ である．また条件（2）より H_2a

$= aH_2$ である．したがって

$$HaH_2aH = Ha^2H_2H = H,$$

$$HaH_2bH_2aH = HH_2abaH_2H = HabaH = HaH$$

である．したがって $HaHaH = H \cup HaH = \bar{G}$ となり $\bar{G} \cdot \bar{G} = \bar{G}$ である．ここで $\{H, a\} \subseteqq H \cup HaH \leqq \langle H, a \rangle$ であるから $G = \bar{G}$ であり，$G_1 = (H \cup HaH)_1 = H$ となり，系 2; 4.8 より $G = H + HaH$ となる．すなわちGはHの可移拡大でΩ上3重可移である．□

この定理を拡張してつぎの系が成り立つ．

系 1.2 $\Omega = \{t, t-1, \cdots, 1, 1', 2', \cdots, n'\}, \Gamma = \{t, t-1, \cdots, 1\}$ $(t \geqq 3)$ とし，$G^{(2)}$ を集合 $\Gamma - \{1, 2\}$ の $t-2$ 個の文字すべてを固定し，$\{2, 1, 1', 2', \cdots, n'\}$ 上の2重可移群とする．

Ω上の $t-1$ 個の置換 $a_2, a_3, \cdots, a_t$，ただし

$$a_i{}^\Gamma = (i \ \ i-1), \qquad i = 2, 3, \cdots, t,$$

$$a_2 \in G^{(2)}$$

がつぎの条件をみたすとする．

（1） $a_i{}^2 \in G^{(2)}, \qquad i = 3, 4, \cdots, t,$

$(a_i a_{i-1})^3 \in G^{(2)}, \qquad i = 3, 4, \cdots, t,$

$(a_i a_j)^2 \in G^{(2)}, \qquad i, j = 2, 3, \cdots, t, \ |i-j| > 1,$

（2） $(G^{(2)}{}_2)^{a_i} = G^{(2)}{}_2, \ \ i = 3, 4, \cdots, t.$

このとき

$$G^{(i+1)} = G^{(i)} + G^{(i)} a_{i+1} G^{(i)}$$

により $i=2$ よりはじめて順次 $G^{(3)}, G^{(4)}, \cdots, G^{(t)}$ を定義すると，$G^{(t)}$ はΩ上 t 重可移群で $G^{(t)}{}_{t\,t-1 \cdots 3} = G^{(2)}$ である．

［証 明］ t に関する帰納法で証明する．

$t=3$ のとき定理 1.1 より成り立つ．

$t \geqq 4$ とし，$i < t$ なる i に対して $G^{(i)}$ は $\{i, \cdots, 1, 1', \cdots, n'\}$ 上 i 重可移で，$G^{(i)}{}_{i \cdots 3} = G^{(2)}$ と仮定する．このとき $G^{(t-1)}, a_t, a_{t-1}$ が定理 1.1 の条件をみたすことを示せばよい．

$$a_t{}^2 \in G^{(2)} \leqq G^{(t-1)}, \qquad (a_t a_{t-1})^3 \in G^{(2)} \leqq G^{(t-1)}$$

であるから，定理 1.1 の条件（1）をみたす．$G^{(2)}{}_2 = G^{(1)}$ とおくと，$G^{(2)} = \langle G^{(1)}, a_2 \rangle$

であり，帰納法の仮定より $G^{(t-1)}{}_{t-1}=G^{(t-2)}$ である．したがって

$$(G^{(t-1)}{}_{t-1})^{a_t}=(G^{(t-2)})^{a_t}=\langle G^{(1)},a_2,\cdots,a_{t-2}\rangle^{a_t}$$

である．ここで条件（2）より $(G^{(1)})^{a_t}=G^{(1)}$ であり，$2\leqq i\leqq t-2$ である a_i に対して条件（1）より $(a_ta_i)^2\in G^{(2)}$ である．したがって $a_t^{-1}a_ia_t\in a_t^{-2}G^{(2)}a_i^{-1}$ となり，$a_t^2\in G^{(2)}\leqq G^{(t-2)}, a_i^{-1}\in G^{(t-2)}$ であるから，$a_t^{-1}a_ia_t\in G^{(t-2)}$, $(G^{(t-2)})^{a_t}=G^{(t-2)}$ となり，定理 1.1 の条件（2）をみたす．したがって定理 1.1 より $G^{(t)}{}_t=G^{(t-1)}$ となり，帰納法の仮定より，$G^{(t)}$ は Ω 上 t 重可移で $G^{(t)}{}_{t\cdots 3}=G^{(2)}$ である．□

この系 1.2 の多重可移群の構成方法にしたがって Mathieu 群を構成する．

定 理 1.3　Ω を $GF(9)$ の 9 元と I, II, ∞ からなる集合，ρ を $\rho^2=2\rho+1$ をみたす $GF(9)^*$ の生成元とし，Ω 上のつぎの置換を作る．

$G^{(2)}$; I, II, ∞ を固定し $GF(9)$ 上 $\Gamma F(9)$ の部分群 $\{\xi\mapsto\rho^i\xi+\alpha\ (i=0,2,4,6),\ \xi\mapsto\rho^i\xi^3+\alpha\ (i=1,3,5,7)\mid\xi,\alpha\in GF(9)\}$,

a_3; I, II を固定し $GF(9)\cup\{\infty\}$ 上 $\Gamma F(9)$ の元 $\xi\mapsto\xi^{-1}$,

a_4; I を固定し，II $\leftrightarrow\infty$, $\xi\mapsto\rho^2\xi+\rho\xi^3$ $(\xi\in GF(9))$,

a_5; I $\leftrightarrow$ II で $GF(9)\cup\{\infty\}$ 上 $\Gamma F(9)$ の元 $\xi\mapsto\xi^3$.

このとき　$G^{(3)}=\langle G^{(2)},a_3\rangle$, $G^{(4)}=\langle G^{(3)},a_4\rangle$, $G^{(5)}=\langle G^{(4)},a_5\rangle$　とおくと，$G^{(i+1)}$ は $G^{(i)}$ の可移拡大で $(i=2,3,4)$，特に $G^{(5)}$ は Ω 上 5 重可移である．

［証 明］ $G^{(2)}$ は明らかに $GF(9)$ 上 $\Gamma F(9)$ の部分群となり，ρ^i と α のとり方より $|G^{(2)}|=9\cdot 8$ である．ここで $GF(9)^*$ の元は $\rho^2=2\rho+1$ より，$\rho^3=2\rho+2, \rho^4=2$, $\rho^5=2\rho, \rho^6=\rho+2, \rho^7=\rho+1$ である．

$G^{(2)}$ の元 $a_2;\xi\mapsto\rho^4\xi+1$ をとると Ω 上

$$a_2=(\mathrm{I})(\mathrm{II})(\infty)(0\ 1)(\rho\ \rho^2)(\rho^3\ \rho^6)(\rho^4)(\rho^5\ \rho^7)$$

である．また

$$G^{(2)}{}_0=\{\xi\mapsto\rho^i\xi\ (i=0,2,4,6),\ \xi\mapsto\rho^i\xi^3\ (i=1,3,5,7)\}$$

で位数は 8 である．したがって $G^{(2)}{}_0$ の元 $b_1;\xi\mapsto\rho\xi^3$, $b_2;\xi\mapsto\rho^2\xi$ をとると，$G^{(2)}{}_0=\langle b_1,b_2\rangle$ で b_1,b_2 は Ω 上

$$b_1=(\mathrm{I})(\mathrm{II})(\infty)(0)(1\ \rho\ \rho^4\ \rho^5)(\rho^2\ \rho^7\ \rho^6\ \rho^3),$$

$$b_2=(\mathrm{I})(\mathrm{II})(\infty)(0)(1\ \rho^2\ \rho^4\ \rho^6)(\rho\ \rho^3\ \rho^5\ \rho^7)$$

である．また a_3,a_4,a_5 は Ω 上

$$a_3=(\mathrm{I})(\mathrm{II})(\infty\ 0)(1)(\rho\ \rho^7)(\rho^2\ \rho^6)(\rho^3\ \rho^5)(\rho^4),$$

$$a_4 = (\mathrm{I})(\mathrm{II}\ \infty)(0)(1)(\rho\ \rho^2)(\rho^3\ \rho^7)(\rho^4)(\rho^5\ \rho^6),$$

$$a_5 = (\mathrm{I}\ \mathrm{II})(\infty)(0)(1)(\rho\ \rho^3)(\rho^2\ \rho^6)(\rho^4)(\rho^5\ \rho^7)$$

である．このとき $G^{(2)}{}_0 = \langle b_1, b_2\rangle, a_2, a_3, a_4, a_5$ が定理 1.2 の条件 (1), (2) をみたすことは，つぎのように容易に示される．

（1） a_3, a_4, a_5 は位数 2 であり，a_2a_3, a_3a_4, a_4a_5 は位数 3 である．さらに a_2 と a_4, a_5 および a_3 と a_5 は可換である．

（2） $b_1^{a_i}, b_2^{a_i} \in G^{(2)}{}_0$ であるから，$(G^{(2)}{}_0)^{a_i} = G^{(2)}{}_0$ である ($i = 3, 4, 5$)．

したがって$G^{(i+1)}$ は $G^{(i)}(i = 2, 3, 4)$ の可移拡大で，$G^{(5)}$ はΩ上 5 重可移である． □

定理 1.3 の 5 重可移群 $G^{(5)}$ を 12 次の **Mathieu 群** M_{12}，4 重可移群 $G^{(4)}$ を 11 次の **Mathieu 群** M_{11} という．

系 1.4 Gを $\Omega=\{1, 2, \cdots, 12\}$ 上の Mathieu 群 M_{12}，$H = G_{1\,2\,3\,4}$ とする．いまΩ上の置換 $b_1, b_2, a_2, a_3, a_4, a_5$ をつぎのように定義するとき，$H = \langle b_1, b_2\rangle$ は 4 元数群で，$\{5, 6, \cdots, 12\}$ 上正則であり

$$M_{11} = \langle H, a_2, a_3, a_4\rangle,$$

$$M_{12} = \langle H, a_2, a_3, a_4, a_5\rangle$$

である．

$$b_1 = (1)(2)(3)(4)(5\ 7\ 6\ 8)(9\ 11\ 10\ 12),$$

$$b_2 = (1)(2)(3)(4)(5\ 9\ 6\ 10)(7\ 12\ 8\ 11),$$

$$a_2 = (1)(2)(3)(4\ 5)(6)(7\ 9)(8\ 11)(10\ 12),$$

$$a_3 = (1)(2)(3\ 4)(5)(6)(7\ 11)(8\ 12)(9\ 10),$$

$$a_4 = (1)(2\ 3)(4)(5)(6)(7\ 9)(8\ 10)(11\ 12),$$

$$a_5 = (1\ 2)(3)(4)(5)(6)(7\ 12)(8\ 11)(9\ 10).$$

ここで4 元数群は問 2；1.4 で求めたが，一般につぎの関係式をもつ位数 8 の群をいう．

$$\langle a, b \mid a^2 = b^2, b^{-1}ab = a^{-1}\rangle.$$

［証 明］ 定理 1.3 の I, II, ∞ および $GF(9)$ の元につぎのように番号をうつ．

$1 = \mathrm{I}$,　$2 = \mathrm{II}$,　$3 = \infty$,　$4 = 0$,　$5 = \rho^0$,　$6 = \rho^4$,　$7 = \rho$,　$8 = \rho^5$,
$9 = \rho^2$,　$10 = \rho^6$,　$11 = \rho^7$,　$12 = \rho^3$.

このとき定理 1.3 および証明で用いた $b_1, b_2, a_2, a_3, a_4, a_5$ は $\Omega = \{1, 2, \cdots, 12\}$ 上定理の形の置換になる．

これより $H=\langle b_1, b_2\rangle$は$\{5, 6, \cdots, 12\}$上正則な4元数群になり，$M_{11}=\langle H, a_2, a_3, a_4\rangle$，$M_{12}=\langle H, a_2, a_3, a_4, a_5\rangle$ である．□

系 1.5 Gを $\Omega=\{1, 2, \cdots, 12\}$ 上の Mathieu 群 M_{12} とする．このとき $\Omega-\{1,2\}$ 上の置換群として $G_{(1,2)}=P\Gamma L(2,9)$ であり，$G_{1\,2}$ は $PSL(2,9)$ を指数2の正規部分群として含む．

［**証 明**］ 定理1.3および系1.4の元を用い，$G_{(1,2)}$ および a_5 の $\Omega-\{1,2\}=\{\infty\}\cup GF(9)$ 上への制限を $\overline{G_{(1,2)}}$, $\bar{a}_5$ とおく．このとき $\langle G^{(2)}, a_3, \bar{a}_5\rangle$ は $\{\infty\}\cup GF(9)$ 上 $\Gamma F(9)$ の部分群である．したがって位数より $\langle G^{(2)}, a_3, \bar{a}_5\rangle=\Gamma F(9)$ である．定理 2; 10.8 より $\Omega-\{1,2\}$ 上 $\Gamma F(9)=P\Gamma L(2,9)$ であり，$\langle G^{(2)}, a_3, \bar{a}_5\rangle=\overline{G_{(1,2)}}$, $\overline{G_{(1,2)}}\cong G_{(1,2)}$ であるから，$\Omega-\{1,2\}$ 上の置換群として，$G_{(1,2)}=P\Gamma L(2,9)$ である．

$G_{1\,2}$ は $G_{(1,2)}$ の指数2の正規部分群である．また $PSL(2,9)$ は $P\Gamma L(2,9)$ の指数4の正規部分群で，定理 2; 10.10 より単純群である．いま $\Omega-\{1,2\}$ 上の置換群として $N=PSL(2,9)$ とおく．

$N\not\leqq G_{1\,2}$ であれば，$\overline{G_{(1,2)}}=G_{1\,2}\cdot N$ である．したがって $\overline{G_{(1,2)}}/G_{1\,2}=G_{1\,2}\cdot N/G_{1\,2}\cong N/G_{1\,2}\cap N$ となりNは指数2の正規部分群 $G_{1\,2}\cap N$ をもつことになり，Nが単純群であることに反する．したがって $N\leqq G_{1\,2}$ で位数よりNは $G_{1\,2}$ の指数2の部分群である．

なお $b_2; \xi\mapsto\rho^2\xi, a_2; \xi\mapsto\rho^4\xi+1, a_3; \xi\mapsto\xi^{-1}$ により，$PSL(2,9)=\langle b_2, a_2, a_3\rangle$ となることが容易にたしかめられる．□

定 理 1.6 Ωを射影空間 $PG(2,4)$ の 21 点と文字 1, 2, 3 からなる集合とし，乗法群 $GF(4)^*$ の生成元を ρ, $PG(2,4)$ の点を $[\lambda_1, \lambda_2, \lambda_3]$ ($\lambda_i\in GF(4)$) で表す．いまΩ上のつぎの置換を作る．

$G^{(2)}$; 1, 2, 3 を固定し $PG(2,4)$ 上 $PSL(3,4)$,

a_3; 1, 2 を固定し，$3\leftrightarrow[1,0,0]$，残りの $PG(2,4)$ の点に対して
$[\lambda_1, \lambda_2, \lambda_3]\mapsto[\lambda_1{}^2+\lambda_2\lambda_3, \lambda_2{}^2, \lambda_3{}^2]$,

a_4; 1を固定し，$2\leftrightarrow 3$,　$[\lambda_1, \lambda_2, \lambda_3]\mapsto[\lambda_1{}^2, \lambda_2{}^2, \rho\lambda_3{}^2]$,

a_5; 3を固定し，$1\leftrightarrow 2$,　$[\lambda_1, \lambda_2, \lambda_3]\mapsto[\lambda_1{}^2, \lambda_2{}^2, \lambda_3{}^2]$.

このとき $G^{(3)}=\langle G^{(2)}, a_3\rangle$, $G^{(4)}=\langle G^{(3)}, a_4\rangle$, $G^{(5)}=\langle G^{(4)}, a_5\rangle$ とおくと，$G^{(i+1)}$ は $G^{(i)}$ の可移拡大で ($i=2,3,4$)，特に $G^{(5)}$ はΩ上5重可移である．

［**証 明**］ $G^{(2)}$ は定理 2;10.5 より $PG(2,4)$ 上2重可移で，定理 2;10.4 より

$$|PG(2,4)| = (4^3-1)/(4-1) = 21,$$
$$|PSL(3,4)| = (4^3-1)(4^3-4)(4^3-4^2)/(4-1)\cdot 3 = 21\cdot 20\cdot 48$$

である．$G^{(2)}$ の元 a_2; $[\lambda_1,\lambda_2,\lambda_3]\mapsto[\lambda_2,\lambda_1,\lambda_3]$ をとる．このとき定理 1.2 の条件 (1), (2) をみたすことを示す．

ここで $PG(2,4)$ の点につぎのように番号をうつ．

$4=[1,0,0]$, $5=[0,1,0]$, $6=[1,1,0]$, $7=[1,\rho,0]$, $8=[1,\rho^2,0]$,
$9=[0,0,1]$, $10=[1,0,1]$, $11=[1,0,\rho^2]$, $12=[1,0,\rho]$, $13=[1,1,1]$,
$14=[0,1,1]$, $15=[1,\rho,\rho]$, $16=[1,\rho^2,\rho^2]$, $17=[1,1,\rho]$, $18=[1,\rho,\rho^2]$,
$19=[1,\rho^2,1]$, $20=[0,1,\rho]$, $21=[1,1,\rho^2]$, $22=[1,\rho^2,\rho]$, $23=[0,1,\rho^2]$,
$24=[1,\rho,1]$.

これにより

$$a_2=(1)(2)(3)(4\ 5)(6)(7\ 8)(9)(10\ 14)(11\ 23)(12\ 20)(13)$$
$$\cdot(15\ 19)(16\ 24)(17)(18\ 22)(21),$$
$$a_3=(1)(2)(3\ 4)(5)(6)(7\ 8)(9)(10)(11\ 12)(13\ 14)(15)(16)$$
$$\cdot(17\ 24)(18\ 23)(19\ 21)(20\ 22),$$
$$a_4=(1)(2\ 3)(4)(5)(6)(7\ 8)(9)(10\ 12)(11)(13\ 17)(14\ 20)$$
$$\cdot(15\ 19)(16\ 18)(21)(22\ 24)(23),$$
$$a_5=(1\ 2)(3)(4)(5)(6)(7\ 8)(9)(10)(11\ 12)(13)(14)(15\ 16)$$
$$\cdot(17\ 21)(18\ 22)(19\ 24)(20\ 23)$$

となる．したがって $a_3^2=a_4^2=a_5^2=1$, $(a_3a_2)^3=(a_4a_3)^3=(a_5a_4)^3=1$, $(a_2a_4)^2=(a_2a_5)^2=(a_3a_5)^2=1$ となり定理 1.2 の条件（1）をみたす．

任意の $[\alpha_{ij}]\in G^{(2)}{}_4$ をとると

$$[1,0,0]^{[\alpha_{ij}]}=[\alpha_{11},\alpha_{12},\alpha_{13}]=[1,0,0]$$

より，$\alpha_{11}=1,\alpha_{12}=\alpha_{13}=0$ としてよい．すなわち

$$G^{(2)}{}_4=\left\{\begin{bmatrix}1&0&0\\ \alpha_{21}&\alpha_{22}&\alpha_{23}\\ \alpha_{31}&\alpha_{32}&\alpha_{33}\end{bmatrix}\middle|\ \alpha_{22}\alpha_{33}+\alpha_{23}\alpha_{32}=1\right\}$$

である．任意の $a=\begin{bmatrix}1&0&0\\ \alpha_1&\alpha_2&\alpha_3\\ \beta_1&\beta_2&\beta_3\end{bmatrix}\in G^{(2)}{}_4$ に対して $a_i^{-1}aa_i$ $(i=3,\ 4,\ 5)$ は 1, 2, 3, 4 を固定する．さらに $[\lambda_1,\lambda_2,\lambda_3]\in PG(2,4)-\{[1,0,0]\}$ に対して

$$a_3^{-1}aa_3;\ [\lambda_1,\lambda_2,\lambda_3]\overset{a_3^{-1}}{\longmapsto}[\lambda_1^2+\lambda_2\lambda_3,\ \ \lambda_2^2,\ \ \lambda_3^2]$$

$$\overset{a}{\longmapsto}[\lambda_1^2+\lambda_2\lambda_3+\alpha_1\lambda_2^2+\beta_1\lambda_3^2,\ \alpha_2\lambda_2^2+\beta_2\lambda_3^2,\ \alpha_3\lambda_2^2+\beta_3\lambda_3^2]$$

$$\overset{a_3}{\longmapsto}[\lambda_1+\lambda_2^2\lambda_3^2+\alpha_1^2\lambda_2+\beta_1^2\lambda_3+\alpha_2\alpha_3\lambda_2+\alpha_2\beta_3\lambda_2^2\lambda_3^2+\beta_2\alpha_3\lambda_2^2\lambda_3^2+\beta_2\beta_3\lambda_3,$$
$$\alpha_2^2\lambda_2+\beta_2^2\lambda_3,\ \alpha_3^2\lambda_2+\beta_3^2\lambda_3]$$
$$=[\lambda_1+(\alpha_1^2+\alpha_2\alpha_3)\lambda_2+(\beta_1^2+\beta_2\beta_3)\lambda_3+(1+\alpha_2\beta_3+\beta_2\alpha_3)\lambda_2^2\lambda_3^2,$$
$$\alpha_2^2\lambda_2+\beta_2^2\lambda_3,\ \alpha_3^2\lambda_2+\beta_3^2\lambda_3]$$
$$=[\lambda_1+(\alpha_1^2+\alpha_2\alpha_3)\lambda_2+(\beta_1^2+\beta_2\beta_3)\lambda_3,\ \alpha_2^2\lambda_2+\beta_2^2\lambda_3,\ \alpha_3^2\lambda_2+\beta_3^2\lambda_3]$$

である．したがって

$$a_3^{-1}aa_3=\begin{bmatrix}1 & 0 & 0\\ \alpha_1^2+\alpha_2\alpha_3 & \alpha_2^2 & \alpha_3^2\\ \beta_1^2+\beta_2\beta_3 & \beta_2^2 & \beta_3^2\end{bmatrix}$$

となり，$\alpha_2^2\beta_3^2+\beta_2^2\alpha_3^2=(\alpha_2\beta_3+\beta_2\alpha_3)^2=1$ より $a_3^{-1}aa_3\in G^{(2)}{}_4$ である．すなわち $(G^{(2)}{}_4)^{a_3}=G^{(2)}{}_4$ が成り立つ．つぎに

$$a_4^{-1}aa_4;[\lambda_1,\lambda_2,\lambda_3]\overset{a_4^{-1}}{\longmapsto}[\lambda_1^2,\lambda_2^2,\rho\lambda_3^2]$$
$$\overset{a}{\longmapsto}[\lambda_1^2+\alpha_1\lambda_2^2+\rho\beta_1\lambda_3^2,\ \alpha_2\lambda_2^2+\rho\beta_2\lambda_3^2,\ \alpha_3\lambda_2^2+\rho\beta_3\lambda_3^2]$$
$$\overset{a_4}{\longmapsto}[\lambda_1+\alpha_1^2\lambda_2+\rho^2\beta_1^2\lambda_3,\ \alpha_2^2\lambda_2+\rho^2\beta_2^2\lambda_3,\ \rho\lambda_3^2\lambda_2+\beta_3^2\lambda_3]$$

である．したがって

$$a_4^{-1}aa_4=\begin{bmatrix}1 & 0 & 0\\ \alpha_1^2 & \alpha_2^2 & \rho\alpha_3^2\\ \rho^2\beta_1^2 & \rho^2\beta_2^2 & \beta_3^2\end{bmatrix}$$

となり，$\alpha_2^2\beta_3^2+\rho^3\beta_2^2\alpha_3^2=1$ より $a_4^{-1}aa_4\in G^{(2)}{}_4$ である．すなわち $(G^{(2)}{}_4)^{a_4}=G^{(2)}{}_4$ が成り立つ．さらに

$$a_5^{-1}aa_5;\ [\lambda_1,\lambda_2,\lambda_3]\overset{a_5^{-1}}{\longmapsto}[\lambda_1^2,\lambda_2^2,\lambda_3^2]$$
$$\overset{a}{\longmapsto}[\lambda_1^2+\alpha_1\lambda_2^2+\beta_1\lambda_3^2,\ \alpha_2\lambda_2^2+\beta_2\lambda_3^2,\ \alpha_3\lambda_2^2+\beta_3\lambda_3^2]$$
$$\overset{a_5}{\longmapsto}[\lambda_1+\alpha_1^2\lambda_2+\beta_1^2\lambda_3,\ \alpha_2^2\lambda_2+\beta_2^2\lambda_3,\ \alpha_3^2\lambda_2+\beta_3^2\lambda_3]$$

である．したがって

$$a_5^{-1}aa_5=\begin{bmatrix}1 & 0 & 0\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2\\ \beta_1^2 & \beta_2^2 & \beta_3^2\end{bmatrix}$$

となり $\alpha_2^2\beta_3^2+\beta_2^2\alpha_3^2=1$ より $a_5^{-1}aa_5\in G^{(2)}{}_4$ である．すなわち $(G^{(2)}{}_4)^{a_5}=(G^{(2)}{}_4)$ が成り立つ．

以上より定理 1.2 の条件（2）をみたし，$G^{(i+1)}$ は $G^{(i)}$ の可移拡大で $(i=2,3,4)$，$G^{(5)}$ は Ω 上 5 重可移である．□

定理 1.6 の 5 重可移群 $G^{(5)}$ を 24 次の **Mathieu 群** M_{24}, 4 重可移群 $G^{(4)}$ を 23 次の **Mathieu 群** M_{23}, 3 重可移群 $G^{(3)}$ を 22 次の **Mathieu 群** M_{22} という.

補 題 1.7　M_{24} の 5 点の安定化群を H とする.

（1） $|H|=2^4\cdot 3$ である.

（2） P を H の 2–シロー部分群とすると, P は H の位数 2^4 の正規部分群で, 8 点を固定する.

（3） Q を H の 3–シロー部分群とすると, 位数は 3 で, 6 点を固定する.

［**証 明**］ $PSL(3,4)$ の位数は $21\cdot 20\cdot 48$ で, $PG(2,4)$ 上 2 重可移である. H は $PSL(3,4)$ における 2 点の安定化群であるから, 位数は $48=3\cdot 2^4$ である. $PSL(3,4)$ は 2 重可移だから, 2 点の安定化群はすべて $PSL(3,4)$ で共役となり, したがって H を 2 点 $[1,0,0]$, $[0,1,0]$ の安定化群としてよい.

定理 1.3 の証明より H は $G^{(2)}{}_4=\left\{\begin{bmatrix}1&0&0\\ \alpha_1&\alpha_2&\alpha_3\\ \beta_1&\beta_2&\beta_3\end{bmatrix}\middle|\ \alpha_2\beta_3+\beta_2\alpha_3=1\right\}$ における $[0,1,0]$ の安定化群である. ここで

$$[0,1,0]^{\begin{bmatrix}1&0&0\\ \alpha_1&\alpha_2&\alpha_3\\ \beta_1&\beta_2&\beta_3\end{bmatrix}}=[\alpha_1,\alpha_2,\alpha_3]=[0,1,0]$$

とすると, $\alpha_1=\alpha_3=0$, $\alpha_2\neq 0$ であり $\alpha_2\beta_3+\beta_2\alpha_3=0$ より $\beta_3=\alpha_2{}^{-1}$ である. したがって

$$H=\left\{\begin{bmatrix}1&0&0\\ 0&\alpha&0\\ \beta&\gamma&\alpha^{-1}\end{bmatrix}\middle|\ \alpha(\neq 0),\beta,\gamma\in GF(4)\right\}$$

である.

H における $[1,1,0]$ の安定化群をとる.

$$[1,1,0]^{\begin{bmatrix}1&0&0\\ 0&\alpha&0\\ \beta&\gamma&\alpha^{-1}\end{bmatrix}}=[1,\alpha,0]=[1,1,0]$$

より $\alpha=1$ である. このとき

$$\left\{\begin{bmatrix}1&0&0\\ 0&1&0\\ \beta&\gamma&1\end{bmatrix}\middle|\ \beta,\gamma\in GF(4)\right\}$$

は位数 2^4 になり, H の位数 $3\cdot 2^4$ であるから H の 2–シロー部分群である. これを P とおくと

$$\begin{bmatrix}1&0&0\\0&1&0\\\beta&\gamma&1\end{bmatrix}^2=\begin{bmatrix}1&0&0\\0&1&0\\2\beta&2\gamma&1\end{bmatrix}=1$$

よりPの元（$\neq 1$）は位数がすべて2になり，Pは基本可換群である．いま

$$[\lambda_1,\lambda_2,\lambda_3]\begin{bmatrix}1&0&0\\0&1&0\\\beta&\gamma&1\end{bmatrix}=[\lambda_1+\beta\lambda_3,\lambda_2+\gamma\lambda_3,\lambda_3]=[\lambda_1,\lambda_2,\lambda_3]$$

とする．$\lambda_3=0$ のとき λ_1,λ_2 の値に関係なく上式は成立し，Pの元はすべて $[\lambda_1,\lambda_2,0]$ を固定する．すなわちPの元はすべて $[1,\lambda,0]$（$\lambda\in GF(4)$）および $[0,1,0]$ の5点を固定する．$\lambda_3\neq 0$ のとき上式は $\beta=\gamma=0$ となり，P の単位元を除く元は $[\lambda_1,\lambda_2,\lambda_3]$（$\lambda_3\neq 0$）を固定しない．以上より$P$は$\Omega$の8点を固定し，$\Omega-F(P)$ 上半正則である．さらに $|\Omega-F(P)|=|P|=2^4$ であるからPは正則である．

つぎにHの部分群

$$Q=\left\{\begin{bmatrix}1&0&0\\0&\alpha&0\\0&0&\alpha^{-1}\end{bmatrix}\middle|\ \alpha\in GF(4)^\prime\right\}$$

をとると，$|Q|=3$ となり，$|H|=3\cdot 2^4$ よりQはHの3-シロー部分群である．いま

$$[\lambda_1,\lambda_2,\lambda_3]\begin{bmatrix}1&0&0\\0&\alpha&0\\0&0&\alpha^{-1}\end{bmatrix}=[\lambda_1,\alpha\lambda_2,\alpha^{-1}\lambda_3]=[\lambda_1,\lambda_2,\lambda_3]$$

とする．$\lambda_1=0$ のとき $[0,\lambda_2,\lambda_3]=[0,\alpha\lambda_2,\alpha^{-1}\lambda_3]=[0,\lambda_2,\alpha^{-2}\lambda_3]$ より，Qの元はすべて $[0,1,0],[0,0,1]$ を固定する．

$\lambda_1\neq 0$ のとき，$\lambda_2=\alpha\lambda_2,\lambda_3=\alpha^{-1}\lambda_3$ よりQの元はすべて $[1,0,0]$ を固定する．以上よりQはΩの6点を固定する．

位数より $H=PQ$ である．さらに任意の$\begin{bmatrix}1&0&0\\0&1&0\\\beta&\gamma&1\end{bmatrix}\in P$，任意の$\begin{bmatrix}1&0&0\\0&\alpha&0\\0&0&\alpha^{-1}\end{bmatrix}\in Q$ に対して

$$\begin{bmatrix}1&0&0\\0&\alpha&0\\0&0&\alpha^{-1}\end{bmatrix}^{-1}\begin{bmatrix}1&0&0\\0&1&0\\\beta&\gamma&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&\alpha&0\\0&0&\alpha^{-1}\end{bmatrix}=\begin{bmatrix}1&0&0\\0&1&0\\\alpha\beta&\alpha^2\gamma&1\end{bmatrix}\in P$$

であるから，PはHの正規部分群である．□

系 1.8 Gを $\Omega=\{1,2,\cdots,24\}$ 上の Mathieu 群 M_{24}, $H=G_{1\,2\,3\,4\,5}$, PをHの2-シロー部分群とする．

Ω上の置換 $b_1,b_2,b_3,b_4,c,a_1,a_2,a_3,a_4,a_5$ をつぎのように定義するとき，

$$P=\langle b_1,b_2,b_3,b_4\rangle,\qquad H=\langle P,c\rangle,$$
$$M_{22}=\langle H,a_1,a_2,a_3\rangle,$$
$$M_{23}=\langle H,a_1,a_2,a_3,a_4\rangle,$$
$$M_{24}=\langle H,a_1,a_2,a_3,a_4,a_5\rangle$$

である.

$$b_1=(1)(2)\cdots(8)(9\ 10)(11\ 12)(13\ 14)(15\ 16)(17\ 18)(19\ 20)(21\ 22)\cdot(23\ 24),$$
$$b_2=(1)(2)\cdots(8)(9\ 11)(10\ 12)(13\ 15)(14\ 16)(17\ 19)(18\ 20)\cdot(21\ 23)(22\ 24),$$
$$b_3=(1)(2)\cdots(8)(9\ 13)(10\ 14)(11\ 15)(12\ 16)(17\ 21)(18\ 22)(19\ 23)\cdot(20\ 24),$$
$$c\ =(1)(2)\cdots(5)(6\ 7\ 8)(9)(10\ 11\ 12)(13\ 18\ 22)(14\ 20\ 23)\cdot(15\ 19\ 21)(16\ 17\ 24),$$
$$a_1=(1)(2)(3)(4)(5\ 9)(6\ 10)(7\ 12)(8\ 11)(13)(14)(15)(16)(17\ 24)\cdot(18\ 22)(19\ 21)(20\ 23),$$
$$a_2=(1)(2)(3)(4\ 5)(6)(7\ 8)(9)(10\ 14)(11\ 23)(12\ 20)(13)(15\ 19)\cdot(16\ 24)(17)(18\ 22)(21),$$
$$a_3=(1)(2)(3\ 4)(5)(6)(7\ 8)(9)(10)(11\ 12)(13\ 14)(15)(16)(17\ 24)\cdot(18\ 23)(19\ 21)(20\ 22),$$
$$a_4=(1)(2\ 3)(4)(5)(6)(7\ 8)(9)(10\ 12)(11)(13\ 17)(14\ 20)(15\ 19)\cdot(16\ 18)(21)(22\ 24)(23),$$
$$a_5=(1\ 2)(3)(4)(5)(6)(7\ 8)(9)(10)(11\ 12)(13)(14)(15\ 16)(17\ 21)\cdot(18\ 22)(19\ 24)(20\ 23).$$

［証 明］ 定理 1.6 の証明と同じようにΩに番号をうつ. 補題 1.7 より

$$H=\left\{\begin{bmatrix}1&0&0\\0&\alpha&0\\\beta&\gamma&\alpha^{-1}\end{bmatrix}\middle|\,\alpha(\neq 0),\beta,\gamma\in GF(4)\right\},\qquad P=\left\{\begin{bmatrix}1&0&0\\0&1&0\\\beta&\gamma&1\end{bmatrix}\middle|\,\beta,\gamma\in GF(4)\right\}$$

である. Pは位数 2^4 の基本可換群だからPの元

$$b_1=\begin{bmatrix}1&0&0\\0&1&0\\1&0&1\end{bmatrix};\ [\lambda_1,\lambda_2,\lambda_3]\longmapsto[\lambda_1+\lambda_3,\lambda_2,\lambda_3]$$

$$b_2=\begin{bmatrix}1&0&0\\0&1&0\\\rho&0&1\end{bmatrix};\ [\lambda_1,\lambda_2,\lambda_3]\longmapsto[\lambda_1+\rho\lambda_3,\lambda_2,\lambda_3]$$

$$b_3=\begin{bmatrix}1&0&0\\0&1&0\\1&1&1\end{bmatrix};\ [\lambda_1,\lambda_2,\lambda_3]\longmapsto[\lambda_1+\lambda_3,\lambda_2+\lambda_3,\lambda_3]$$

$$b_4=\begin{bmatrix}1&0&0\\0&1&0\\\rho^2&\rho^2&1\end{bmatrix};\ [\lambda_1,\lambda_2,\lambda_3]\longmapsto[\lambda_1+\rho^2\lambda_3,\lambda_2+\rho^2\lambda_3,\lambda_3]$$

をとると，$P=\langle b_1,b_2,b_3,b_4\rangle$ で，Ω 上定理の置換で書ける．またHの位数 3 の元

$$c=\begin{bmatrix}1&0&0\\0&\rho&0\\0&0&\rho^2\end{bmatrix};\ [\lambda_1,\lambda_2,\lambda_3]\longmapsto[\lambda_1,\rho\lambda_2,\rho^2\lambda_3]$$

をとると，c は定理の置換になり，$H=\langle P,c\rangle$ である．

さらに $PSL(3,4)$ の元

$$a_1=\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix};\ [\lambda_1,\lambda_2,\lambda_3]\longmapsto[\lambda_1,\lambda_3,\lambda_2]$$

および定理 1.6 で用いた a_2,a_3,a_4,a_5 により定理の結果をうる．□

系 1.9　Gを $\Omega=\{1,2,\cdots,24\}$ 上の Mathieu 群 M_{24}，Pを G_{12345} の 2-シロー部分群とすると，$N_G(P)^{F(P)}=A_8$ で，これより $A_8\cong PSL(4,2)$ である．（第 2 章 §8 の問題参照）

［**証 明**］ 系 1.8 の元を用いる．このとき $F(P)=\{1,2,\cdots,8\}$ で補題 1.7 (2) より Pは $\{9,10,\cdots,24\}$ 上正則な位数 16 の基本可換群である．したがって定理 2;9.13 より $\mathrm{Aut}\ P\cong GL(4,2)=PSL(4,2)$である．

PはΩ上 5 重可移群Gにおける 5 点の安定化群 G_{12345} の 2-シロー部分群であるから，定理 2；8.5 より $N_G(P)^{F(P)}$ は $F(P)$ 上 5 重可移群である．さらに補題 1.7 (2) より $P\leqq G_{12345}$ であるから $c\in N_G(P)$ で，$c^{F(P)}=(6\ 7\ 8)$ である．したがって系 2;8.3 より $N_G(P)^{F(P)}\geqq A_8$ である．いま $N_G(P)^{F(P)}=S_8$ であれば；$N_G(P)$ は $a=(1)(2)\cdots(5)(6\ 7)(8)\cdots$ なる位数が 2 のべきの元をもち，$\langle P,a\rangle$ はPを真部分群としてもつ G_{12345} の 2-部分群となり，Pが G_{12345} の 2-シロー部分群であることに反する．したがって $N_G(P)^{F(P)}=A_8$ である．

定理 1;3.5 より $N_G(P)/C_G(P)\leqq\mathrm{Aut}\,P$ である．ここでPは $\Omega-F(P)$ 上正則な可換群であるから，系 2; 11.8 より $C_G(P)$ はPを含み，$\Omega-F(P)$ 上一致する．さらに

$|\Omega - F(P)| = 16$ でGの元（$\neq 1$）は高々 8 点を固定するから $C_G(P)_{\Omega-F(P)} = 1$ で，$C_G(P)^{\Omega-F(P)} \cong C_G(P)/C_G(P)_{\Omega-F(P)} = C_G(P)$ となり，$C_G(P) = P$ である．

以上より $N_G(P)^{F(P)} \cong N_G(P)/N_G(P)_{F(P)} = N_G(P)/P = N_G(P)/C_G(P) \leqq \mathrm{Aut}\,P$ となる．ここで $N_G(P)^{F(P)} = A_8, \mathrm{Aut}\,P = PSL(4,2)$ で $|A_8| = |PSL(4,2)|$ であるから $A_8 \cong PSL(4,2)$ となる．□

定 理 1.10 Mathieu 群 $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ はすべて単純群である．

［**証 明**］ Gを次数nの Mathieu 群 M_n $(n = 11, 12, 22, 23, 24)$ とすると，Gは 3 重可移だから定理 2;12.2 より正則正規部分群をもたない．

（i） $G = M_{11}$ としNをGの正規部分群（$\neq 1$）とする．定理 2;12.6 よりNは 3 重可移で，$|G| = 11\cdot10\cdot9\cdot8$ より $|N| = 11\cdot10\cdot9\cdot2^k$（$k = 0, 1, 2$ または 3）である．PをNの 11-シロー部分群とすると，GとNの位数よりPはGの 11-シロー部分群であり，位数11の正則な置換群である．

NはGの正規部分群だから，シローの定理（定理 2;6.7）よりGの 11-シロー部分群はすべてNに含まれる．すなわちGとNは同数個の11-シロー部分群を含み，定理 1;2.1 より

$$|G|/|N_G(P)| = |N|/N_N(P),$$
$$|N_G(P)| = (|G|/|N|)\cdot|N_N(P)| = 2^{3-k}\cdot|N_N(P)|$$

である．

いま $k \neq 3$ とすると $|N_G(P)|$ は 2 の倍数となり $N_G(P)$ は位数 2 の元aをもつ．系 1.4 の M_{11} の生成元より M_{11} は偶置換よりなり，したがってaの巡回表示は偶数個の互換よりなる．ここで次数は 11 だから，aは少なくとも 3 点を固定する．このとき系 2;11.5 より $3 \leqq |C_P(a)|$ である．一方 $|P| = 11$ だから $C_P(a) = P$ となり，系 2;11.5 より $|F(a)| = 11$ すなわち $a = 1$ となり，aの位数が 2 であることに反する．

以上より $k = 3$ となり，$G = N$ すなわち $G = M_{11}$ は単純群である．

さらに M_{11} が単純群であるから，定理 2;12.3 より M_{12} も単純群になる．

（ii） $G = M_{22}$ とする．Gは 22 点上 3 重可移で 1 点の安定化群は定理 1.6 より $PSL(3,4)$ である．ここで $PSL(3,4)$ は定理 2;10.10 より単純群だから，定理 2;12.3 より $G = M_{22}$ も単純群になる．

同様にして順次 M_{23}, M_{24} も単純群になる．□

定 理 1.11 12次の Mathieu 群の可移拡大は存在しない．

［**証 明**］ M_{12} の可移拡大Gが存在するとする．すなわちGは $\Omega = \{1, 2, \cdots, 13\}$ 上の

可移群で G_1 は $\{2, 4, \cdots, 13\}$ 上 M_{12} とする．このとき G は Ω 上 6 重可移である．$G_{12345}=H$ とおくと，$|F(H)|=5$ で定理 2; 8.4 より $N_G(H)^{F(H)}$ は 5 重可移となり対称群 S_5 である．したがって $a=(1\ 2\ \cdots\ 5)\cdots$ なる位数が 5 のべきである元 $a\in N_G(H)$ が存在する．ここで $|\Omega-\{1, 2, \cdots, 5\}|=8$ であるから，$|F(a)|=3$ または 8 である．さらに系 1.4 より H は $\{6, 7, \cdots, 13\}$ 上正則で $a\in N_G(H)$ であるから，系 2;11.5 より $|F(a)|=|C_H(a)|$ である．したがって H は 2- 群であるから $|F(a)|=8$ となる．

一方 G は 6 重可移であるから，5 点以上を固定する元は H の元と共役で，a は H の元と共役である．しかし H は 2-群であるから，a の位数が 5 であることに矛盾する．したがって M_{12} の可移拡大は存在しない．□

定 理 1.12　24 次の Mathieu 群 M_{24} の可移拡大は存在しない．

［証 明］ M_{24} の可移拡大 G が存在するとする．すなわち G は $\Omega=\{1, 2, \cdots, 25\}$ 上の可移群で，G_1 は $\{2, 4, \cdots, 25\}$ 上 M_{24} とする．このとき G は 6 重可移であり，P を $G_{12\cdots 6}$ の 2- シロー部分群とする．補題 1.7 (2) より $|F(P)|=9$ で定理 2;8.5 より $N_G(P)^{F(P)}$ は 6 重可移である．したがって系 1.9 より $N_{G_1}(P)^{F(P)-\{1\}}=A_8$ であるから，$N_G(P)^{F(P)}\geqq A_9$ である．

いま $F(P)=\{1, 2, \cdots, 9\}$ とすると，$N_G(P)^{F(P)}\geqq A_9$ より位数が 3 のべきである $a=(1\ 2\ \cdots\ 9)\cdots\in N_G(P)$ が存在する．ここで $|\Omega-\{1, 2, \cdots, 9\}|=16$ であるから a の位数は 3^2 で，$\{10, 11, \cdots, 25\}$ 上 a は高々 1 個の 9- 巡回置換をもち，16点または 7 点よりなる $\{10, 11, \cdots, 25\}$ の部分集合上いくつかの 3-巡回置換と固定点よりなる．したがって，a^3 は位数が 3 で $\{10, 11, \cdots, 25\}$ 上 16 点または 7 点を固定する．一方，$a^3\in N_G(P)$ で P は定理1.7 (2) より $\{10, 11, \cdots, 25\}$ 上正則であるから，系 2; 11. 5 より $|F(a^3)|=|C_H(a^3)|$ である．よって P は 2- 群であるから $|F(a^3)|=16$ となる．

$G_{12\cdots 6}$ の位数 3 の元は補題 1.7 (3) より 7 点を固定し，G は 6 重可移だから 6 点以上の固定点をもつ位数 3 の元はちょうど 7 点を固定する．したがって $|F(a^3)|=16$ はおこりえない．すなわち M_{24} の可移拡大は存在しない．□

§ 2. ウイットシステムの構成

$\Omega, \mathfrak{B}$ を 2 つの集合，I を直積集合 $\Omega\times\mathfrak{B}$ の部分集合とするとき，これら 3 つの集合の組 $(\Omega, \mathfrak{B}, I)$ を**結合構造** (incidence structure) という．このとき Ω の元を**点**，$\mathfrak{B}$ の元を**ブロック**という．

$i\in\Omega$, $B\in\mathfrak{B}$ が $(i, B)\in I$ のとき，iIB と書き，i とBは結合関係にある，i はBの上にある，Bは i を通る，などという．特に$\mathfrak{B}$がΩの部分集合の集合で，点 i とブロックBの結合関係 iIB を $i\in B$ で定義した結合構造を，I をはぶいて $(\Omega,\mathfrak{B})$ と書く．以下の結合構造はすべて $(\Omega,\mathfrak{B})$ とする．

2つの結合構造 $D=(\Omega,\mathfrak{B})$ と $D'=(\Omega',\mathfrak{B}')$ が**同型**であるとは，全単射 $\varphi: D\to D'$ が存在して，$\mathfrak{B}^{\varphi}=\{B^{\varphi}|B\in\mathfrak{B}\}=\mathfrak{B}'$ のときをいう．ここで $B^{\varphi}=\{i^{\varphi}|i\in B\}$ とする．

aが結合構造 $D=(\Omega, \mathfrak{B})$ の**自己同型（写像）**であるとは，aはΩ上の置換で $\mathfrak{B}^{a}=\mathfrak{B}$ のときをいう．さらに自己同型全体は写像の積に関して群を作る．これをDの**（全）自己同型群**といい，Aut D と書く．

つぎの2つの条件をみたす結合構造 $(\Omega, \mathfrak{B})$ を **t-(v, k, λ) デザイン** (t-(v,k,λ) design) という．ただし $|\Omega|=v$ とする．

（1） $\mathfrak{B}$の各ブロックはすべてΩの k 個の点よりなる．

（2） Ωの任意の t 個の点を含むブロックの個数は一定数 λ である．

λを**会合数**という．また t-(v,k,λ) デザインを単に **t-デザイン**ということもある．ここで $v>k\geqq t$ とする．特に $\lambda=1$ の t-$(v, k, 1)$ デザインを**シュタイナーシステム** (Steiner system) ともいい，これを $S(t,k,v)$ と書くときもある．

$D=(\Omega, \mathfrak{B})$ を t-(v,k,λ) デザイン，Δを $|\Delta|=k'<t$ であるΩの部分集合とする．$\mathfrak{B}_{\Delta}=\{B_{\Delta}=B-\Delta|\Delta\subset B\in\mathfrak{B}\}$ とおき，結合構造 $(\Omega-\Delta,\mathfrak{B}_{\Delta})$ をDのΔに関する**内部構造**といい D_{Δ} と書く．また $(t+1)$-$(v+1,k+1,\lambda)$ デザイン $D'=(\Omega',\mathfrak{B}')$ が存在して，$i'\in\Omega'$ に対してDが D' の点 i' に関する内部構造 $D_{i'}$ に同型のとき，D' をDの**拡大**という．

定理 2.1 $D=(\Omega,\mathfrak{B})$ を t-(v,k,λ) デザイン，Δを $|\Delta|=k'<t$ であるΩの部分集合とする．このときDのΔに関する内部構造 D_{Δ} は $(t-k')$-$(v-k',k-k',\lambda)$ デザインである．

［証明］ $|\Omega-\Delta|=v-k'$ で，任意の $B_{\Delta}\in\mathfrak{B}_{\Delta}$ は $|B_{\Delta}|=k-k'$ である．任意の $t-k'$ 個の $\Omega-\Delta$ の点からなる集合Γに対して，$|\Gamma\cup\Delta|=t$ であるから，$\Gamma\cup\Delta$ を含むDのブロックは λ 個存在し，それらは D_{Δ} の異なるブロックを作る．逆にΓを含む D_{Δ} のブロック B_{Δ} をとると，$B_{\Delta}\cup\Delta$ はDのブロックを作る．したがって D_{Δ} の会合数も λ

で D_Δ は $(t-k')$-$(v-k', k-k', \lambda)$ デザインである. □

定理 2.2 GをΩ上の t 重可移群とする. Δを $t \leqq |\Delta| < |\Omega|$ であるΩの部分集合とし, $\mathfrak{B}=\{\Delta^a | a \in G\}$ とおくとき, $(\Omega, \mathfrak{B})$ は t-デザインで, $|\mathfrak{B}| = |G|/|G_{(\Delta)}|$ である.

［証 明］ $\mathfrak{B}$ の元はすべてΩの$|\Delta|$個の点よりなる集合である. また任意の異なる t 個の点を含む$\mathfrak{B}$の元の個数はGが t 重可移だから一定となり, $(\Omega, \mathfrak{B})$ は t-デザインである. さらにGは$\mathfrak{B}$の上に可移に作用するから $|\mathfrak{B}|=|G|/|G_{(\Delta)}|$ である. □

系 2.3 Gを $\Omega=\{1,2,\cdots,n\}$ 上の t 重可移群とする. $\{1,2,\cdots,t\} \subseteqq \Delta \subsetneqq \Omega$ に対して, t-デザイン $D=(\Omega, \mathfrak{B}), \mathfrak{B}=\{\Delta^x | x \in G\}$ を作る.

いま任意の $x \in G$ に対して, $\{1,2,\cdots,t\} \subseteqq \Delta^x$ であればつねに $\Delta^x = \Delta$ が成り立つとき, Dは t-$(n, |\Delta|, 1)$ デザインで, $G_{(\Delta)}$ はΔ上 t 重可移である.

［証 明］ Ωの任意の異なる t 個の点 $i_1, i_2, \cdots, i_t$ をとる. G は Ω 上 t 重可移だから $a=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ i_1 & i_2 & \cdots & i_t & \cdots \end{pmatrix} \in G$ が存在し, $\{i_1, i_2, \cdots, i_t\} \subseteqq \Delta^a$ である. いま $\{i_1, i_2, \cdots, i_t\} \subseteqq \Delta^b \in \mathfrak{B}$とすると, $\{1,2,\cdots,t\} = \{i_1, i_2, \cdots, i_t\}^{a^{-1}} \in \Delta^{ba^{-1}} \in \mathfrak{B}$ である. したがって仮定より $\Delta = \Delta^{ba^{-1}}, \Delta^a = \Delta^b$ となり $\{i_1, i_2, \cdots, i_t\}$ を含むブロックは Δ^a のみである. すなわち会合数 $\lambda=1$ となりDは t-$(n, |\Delta|, 1)$ デザインである.

いまΔの任意の異なる t 個の文字よりなる 2 つの順列 $(j_1, j_2, \cdots, j_t), (j_1', j_2', \cdots, j_t')$ をとるとGは t 重可移だから $(j_1, j_2, \cdots, j_t)^x = (j_1', j_2', \cdots, j_t')$ なる元 $x \in G$ が存在する. このとき $\{j_1', j_2', \cdots, j_t'\} = \{j_1, j_2, \cdots, j_t\}^x \subseteqq \Delta^x$ だから $\Delta^x = \Delta$ である. すなわち $x \in G_{(\Delta)}$ で $G_{(\Delta)}$ はΔ上 t 重可移である. □

Hを群Gの部分群, KをHの部分集合 $(\neq \phi)$ とする. 任意の $x \in G$ に対して $K^x \subseteqq H$ であればつねに $K^x = K$ が成り立つとき, KはHの中で**弱閉**であるという.

系 2.4 Gを $\Omega=\{1,2,\cdots,n\}$上の t 重可移群とし, $H=G_{12\cdots t}$ とする. Hの部分集合 $N(\neq 1)$ がHで弱閉であれば, 結合構造 $(\Omega, \mathfrak{B}), \mathfrak{B}=\{F(N^x) | x \in G\}$ は t-$(n, |F(N)|, 1)$ デザインである.

［証 明］ $1 \neq N \subseteqq H$ より $|\Omega| > |F(N)| \geqq |F(H)| \geqq t$ であり, $x \in G$ に対して $F(N)^x = F(N^x)$ であるから, $(\Omega, \mathfrak{B})$ は定理 2.2 より t-デザインである. いま $\{1,2,\cdots,t\} \subseteqq F(N^x)$ とする. このとき $N^x \subseteqq H$ で, 仮定よりNはHで弱閉であるから $N^x = N$となり, $F(N^x) = F(N)$ である. したがって系 2.3 より $(\Omega, \mathfrak{B})$ は t-$(n, |F(N)|,$

1) デザインである. □

以下, Witt により Mathieu 群からウイットシステムが構成されたが, それについて述べる.

補 題 2.5 Gを $\Omega=\{1,2,\cdots,12\}$ 上の Mathieu 群 M_{12}, aを4点を固定する位数2のGの元とする. いまΔを $F(a)$ の4点とaの巡回表示における任意の1つの互換を作る2点からなる6点の集合とすると, $G_{(\Delta)}$ はΔ上対称群 S_6 である.

［証 明］ 系 1.4 よりGにおける4点の安定化群は4元数群となり, 位数2の元をただ1つもつ. いまaを4点を固定する位数2の元とし

$$a=(1)(2)(3)(4)(5\ 6)\cdots$$

として, $\Delta=\{1,2,\cdots,6\}$ とおく. 1,2,3,4 の任意の順列 (i_1,i_2,i_3,i_4) に対して, Gは5重可移だからGに

$$b=(i_1\ i_2)(i_3)(i_4)(5)\cdots$$

なる元が存在する. このとき $b\in N_G(G_{1234})$ で, aは G_{1234} のただ1つの位数2の元だから, bとaは可換になり, したがって

$$b=(i_1\ i_2)(i_3)(i_4)(5)(6)\cdots$$

となり, bはまた4点を固定して互換 $(i_1\ i_2)$ をもつから, 位数2である.

(i_1,i_2,i_3,i_4) は 1,2,3,4 の任意の順列で, $b\in(G_{(\Delta)})_{56}$ だから $(G_{(\Delta)})_{56}$ は $\{1,2,3,4\}$ 上対称群 S_4 になる. 同様にして $F(b)=\{i_3,\ i_4,5,6\}$ より $(G_{(\Delta)})_{i_1 i_2}$ は $\{i_3,\ i_4,\ 5,6\}$ 上 S_4 になる. したがって $G_{(\Delta)}\geqq\langle(G_{(\Delta)})_{56},(G_{(\Delta)})_{i_1 i_2}\rangle$ であるから $G_{(\Delta)}$ はΔ上 S_6 である. □

定 理 2.6 Gを $\Omega=\{1,2,\cdots,12\}$ 上の Mathieu 群 M_{12}, Iを4点を固定するGの位数2の元すべてよりなる集合とする. 任意の $a=(j_1\ k_1)(j_2\ k_2)\cdot(j_3\ k_3)(j_4\ k_4)\in I$ に対して $\Delta_i(a)=F(a)\cup\{j_i,k_i\}$ $(i=1,2,3,4)$ とおく. このとき $\mathfrak{B}=\{\Delta_i(a)\mid a\in I,\ i=1,2,3,4\}$ とすると, $D=(\Omega,\mathfrak{B})$ は 5-(12, 6,1) デザインである.

同様にして Mathieu 群 M_{11} および M_{12} の2点の安定化群よりそれぞれ 4-(11,5,1) デザイン, 3-(10,4,1) デザインが作られる.

［証 明］ Ωの5点 1,2,3,4,5 をとる. G_{1234} の位数2の元は系 1.4 よりただ1つである. いまこれをaとし

$$a = (1)(2)(3)(4)(5\ 6)\cdots$$

とする．$\varDelta = \{1, 2, \cdots, 6\}$ とおき，$\{1, 2, \cdots, 5\} \subseteqq \varDelta^x$, $x \in G$ とする．このとき $x = \begin{pmatrix} 1 & 2 & \cdots & 6 & \cdots \\ i_1 & i_2 & \cdots & i_6 & \cdots \end{pmatrix}$ で $\varDelta^x = \{i_1, i_2, \cdots, i_6\} = \{1, 2, \cdots, 5, i\}$, $i \in \{6, 7, \cdots, 12\}$ である．したがって

$$a^x = (i_1)(i_2)(i_3)(i_4)(i_5\ i_6)\cdots$$

となる．さらに補題 2.5 より $G_{(\varDelta^x)}$ は $\varDelta^x$ 上対称群 S_6 であるから，$y = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & i_6 & \cdots \\ 1 & 2 & 3 & 4 & 5 & i & \cdots \end{pmatrix} \in G_{(\varDelta^x)}$ が存在して

$$a^{xy} = (1)(2)(3)(4)(5\ i)\cdots$$

となる．ここで $G_{1\,2\,3\,4}$ の位数 2 の元は a のみであるから，$a^{xy} = a$ となり $i = 6$ である．すなわち $\varDelta^x = \varDelta$ である．

したがって系 2.3 より $\mathfrak{B}' = \{\varDelta^x \mid x \in G\}$ をブロックの集合とする 5-(12, 6, 1) デザインをうる．

ここで任意の $\varDelta^x \in \mathfrak{B}'$ に対して，$\varDelta^x = \varDelta_i(a^x)$, $i \in \{1, 2, 3, 4\}$ である．逆に任意の $\varDelta_i(b)$ に対して，G は 5 重可移であるから，$x \in G$ が存在して $\varDelta^x = \varDelta_i(b)$ となる．したがって

$$\mathfrak{B}' = \{\varDelta_i(a) \mid a \in I,\ i = 1, 2, 3, 4\} = \mathfrak{B}$$

である．

同様にして M_{11} または M_{12} の 2 点の安定化群に対して，それぞれ 3 点または 2 点を固定する位数 2 の元をとることにより 4-(11, 5, 1) デザイン，3-(10, 4, 1) デザインをうる．□

定理 2.6 の 5-(12, 6, 1) デザイン，4-(11, 5, 1) デザインは共にシュタイナーシステムで，それぞれウイットシステム W_{12}, W_{11} という．また 3-$(n^2+1, n+1, 1)$ デザインを inversive 平面という．したがって 3-(10, 4, 1) デザインは $n = 3$ のときの inversive 平面である．定理 2.6 でえられた 3-(10, 4, 1) デザインを本書においては W_{10} と書くことにする．また W_{12} は W_{11} の拡大，W_{11} は W_{10} の拡大である．

定 理 2.7 Gを $\Omega = \{1, 2, \cdots, 24\}$ 上の Mathieu 群 M_{24}, S をGの 5 点の安定化群の 2-シロー部分群すべての集合とする．このとき $\mathfrak{B} = \{F(P) \mid P \in S\}$ とおくと，$D = (\Omega, \mathfrak{B})$ は 5-(24, 8, 1) デザインである．

同様にして Mathieu 群 M_{23}, M_{22} よりそれぞれ 4-(23, 7, 1) デザイン，

3-(22, 6, 1) デザインが作られる．

［証 明］ Gは定理 1.6 よりΩ上5重可移である．さらにPを G_{12345} の 2-シロー部分群とすると，補題 1.7 (2) よりPは G_{12345} の正規部分群であるから G_{12345} の 2-シロー部分群はPのみである．したがってPは G_{12345} の弱閉な部分群であり，補題 1.7 (2) より $|F(P)|=8$ であるから，系 2.4 より $\mathfrak{B}'=\{F(P^x)|x\in G\}$ をブロックの集合とする 5-(24, 8, 1) デザインをうる．また明らかに $\{P^x|x\in G\}=S$ であるから $\mathfrak{B}'=\mathfrak{B}$ である．

同様にして M_{23} または M_{22} に対して，それぞれ4点または3点の安定化群の 2-シロー部分群の固定点の集合をとることにより，4-(23, 7, 1) デザイン，3-(22, 6, 1) デザインをうる．□

定理 2.7 の 5-(24, 8, 1) デザイン，4-(23, 7, 1) デザイン，3-(22, 6, 1) デザインはシュタイナーシステムであり，それぞれウイットシステム W_{24}, W_{23}, W_{22} という．また W_{24} は W_{23} の拡大，W_{23} は W_{22} の拡大である．

定 理 2.8 $(\Omega, \mathfrak{B})$ を t-(v, k, λ) デザインとする．このとき $0\leqq s\leqq t$ であるs個の点を通るブロックの個数は，s個の点のとり方にかかわらず一定数

$$r_s=\lambda\cdot\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}=\lambda\cdot\frac{(v-s)\ (v-s-1)\cdots(v-t+1)}{(k-s)\ (k-s-1)\cdots(k-t+1)}$$

である．特に $b=r_0, r=r_1$ とおくとbは$\mathfrak{B}$のブロックの個数，rは1点を通るブロックの個数で

$$vr=bk$$

である．

［証 明］ $0\leqq s\leqq t$ であるΩのs個の異なる点 $i_1, i_2, \cdots, i_s$ を定め，$\bar{\Omega}=\{\Delta|\Delta\subseteqq\Omega-\{i_1, i_2, \cdots, i_s\}, |\Delta|=t-s\}$, $\overline{\mathfrak{B}}=\{B|\{i_1, i_2, \cdots, i_s\}\subseteqq B\in\mathfrak{B}\}$ とおく．ここで $|\overline{\mathfrak{B}}|=r_s$ である．

集合 $S=\{(\Delta, B)|\Delta\in\bar{\Omega},\ B\in\overline{\mathfrak{B}},\ \Delta\subseteqq B\}$ の元の個数を2通りの方法で数える．

Δのとり方は $|\bar{\Omega}|=\binom{v-s}{t-s}$ 通りで，各Δに対して $\Delta\subseteqq B\in\overline{\mathfrak{B}}$ であるブロックBは $\Delta\cup\{i_1, i_2, \cdots, i_s\}$ のt個の点をつねに含むからλ個存在し，したがって$|S|=\binom{v-s}{t-s}\cdot\lambda$ である．

一方Bのとり方は $|\overline{\mathfrak{B}}|=r_s$ 通りで，各Bに対してBに含まれる $\Delta\in\bar{\Omega}$ の個数は

$\binom{k-s}{t-s}$ であるから，$|S| = r_s \cdot \binom{k-s}{t-s}$ である．したがって

$$\binom{v-s}{t-s}\cdot\lambda = r_s\cdot\binom{k-s}{t-s}$$

より

$$r_s = \lambda\cdot\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \lambda\cdot\frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}$$

となり，s 個の点のとり方にかかわらない．

またここで r_0 は $\mathfrak{B}$ のブロックの個数，r_1 は 1 点を通るブロックの個数であるから，上式を用いて

$$b = r_0 = \lambda\ \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)},$$

$$r = r_1 = \lambda\ \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}$$

であるから，$b = r\cdot\dfrac{v}{k}$ となり $vr = bk$ となる．□

定 理 2.9　W_{12} は拡大できない．

［証 明］ W_{12} の拡大 D が存在するとすると，D は 6-(13, 7, 1) デザインである．このとき定理 2.8 より D のブロックの個数は

$$1\cdot\frac{13\cdot12\cdot11\cdot10\cdot9\cdot8}{7\cdot6\cdot5\cdot4\cdot3\cdot2} = \frac{13\cdot12\cdot11}{7}$$

となり整数にならない．したがって拡大 D は存在しない．□

定 理 2.10　W_{24} は拡大できない．

［証 明］ W_{24} の拡大 D が存在するとすると，D は 6-(25, 9, 1) デザインである．このとき定理 2.8 より D のブロックの個数は

$$1\cdot\frac{25\cdot24\cdot23\cdot22\cdot21\cdot20}{9\cdot8\cdot7\cdot6\cdot5\cdot4} = \frac{25\cdot23\cdot22}{3}$$

となり整数にならない．したがって拡大 D は存在しない．□

§3. 射影平面，アフィン平面

つぎの 3 条件をみたす結合構造 $(\Omega, \mathfrak{B})$ を**射影平面** (projective plane) という．ここでブロックを直線という．

（1） 異なる 2 点を通る直線がただ 1 つ存在する．

（2） 異なる 2 直線はただ 1 点を共有する．

（3） いずれの3点も同一直線上にない4点が存在する．なお2直線の共有点を2直線の交点という．

注 3.1 有限体 $GF(q)$ 上の射影平面 $PG(2,q)$ は，点全体の集合を Ω，直線全体の集合を $\mathfrak{B}$ とする結合構造としても，上の定義による射影平面である．

［証 明］（1） $PG(2,q)$ の異なる2点 $[v_1]$, $[v_2]$ $(v_1, v_2 \in V(3,q))$ をとる．v_1, v_2 は $V(3,q)$ で1次独立だから，v_1, v_2 を含む2次元部分ベクトル空間は $\langle v_1, v_2\rangle$ のみである．したがって $[v_1]$, $[v_2]$ を通る $PG(2,q)$ の直線はただ1つ $[\langle v_1, v_2\rangle]$ のみである．

（2） $PG(2,q)$ の異なる2直線 $[U_1], [U_2]$ (U_1, U_2 は $V(3,q)$ の2次元部分ベクトル空間) をとる．U_1, U_2 は3次元ベクトル空間における異なる2次元部分ベクトル空間だから $U_1 \cap U_2$ は1次元部分ベクトル空間である．すなわち $[U_1]$ と $[U_2]$ はただ1点で交わる．

（3） $V(3,q)$ において座標が $(1,0,0), (0,1,0), (0,0,1), (1,1,1)$ の4つのベクトルはいずれの3つも1次独立だから同じ2次元部分ベクトル空間に含まれない．したがって $PG(2,q)$ において4点 $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, $[1,1,1]$ のいずれの3点も同一直線上にない．□

補 題 3.2 2-$(n^2+n+1, n+1, 1)$ デザインにおいて，ブロックの個数は n^2+n+1 個，1点を通るブロックの個数は $n+1$ 個である．

［証 明］ 定理2.8よりブロックの個数は

$$r_0 = 1 \cdot \frac{(n^2+n+1)(n^2+n)}{(n+1)n} = n^2+n+1$$

である．また1点を通るブロックの個数は

$$r_1 = 1 \cdot \frac{n^2+n}{n} = n+1$$

である．□

定 理 3.3 結合構造 $(\Omega, \mathfrak{B})$ が射影平面であることと 2-$(n^2+n+1, n+1, 1)$ デザイン$(n \geqq 2)$ であることとは同じである．

［証 明］（i） $(\Omega, \mathfrak{B})$ を射影平面とし，これが 2-$(n^2+n+1, n+1, 1)$ デザインになることを示す．l を $\mathfrak{B}$ の1つの直線とし，l 上の点の個数を $n+1$ とする．射影平面の条件（3）より l 上にない点が存在するから，p を l 上にない任意の点とする．p を通る任意の直線は l と異なるから条件（2）より l とただ1点で交わる．また l 上の点と p を通る直線は条件（1）よりただ1つ存在する．したがって p を通る直線は $n+1$ 個である．

g を l と異なる任意の直線とする．点 p を l 上にも g 上にもない点としてとることができる．なぜならば Ω の点がすべて g または l 上にあるとすると条件（3）より g と l の交点以外に l 上に 2 点 p_1, p_2, g 上に 2 点 q_1, q_2 が存在し，p_1, q_1 を通る直線と p_2, q_2 を通る直線の交点は g, l 上になく矛盾である．したがって上で示したことより，p を通る直線の個数は $n+1$ 個で g 上の点の個数に等しい．すなわち任意の直線は $n+1$ 個の点を含む．

任意の 2 点を通る直線は条件（1）よりただ 1 つ存在するから，$(\Omega, \mathfrak{B})$ は会合数 $\lambda=1$ の 2- デザインである．

点 p を通る直線は $n+1$ 個存在し，各直線は $n+1$ 個の点を含む．条件（1）より p 以外の Ω の点は p を通るちょうど 1 つの直線に含まれる．したがって Ω の点の個数は $n(n+1)+1=n^2+n+1$ である．また条件（3）より $n \geqq 2$ である．

以上より射影平面は 2-$(n^2+n+1, n+1, 1)$ デザイン $(n \geqq 2)$ である．

（ii） $(\Omega, \mathfrak{B})$ を 2-$(n^2+n+1, n+1, 1)$ デザイン $(n \geqq 2)$ とし，これが射影平面になることを示す．ここで $\mathfrak{B}$ のブロックを直線とよぶことにする．

（1） 会合数 $\lambda=1$ の 2-デザインだから，2 点を通る直線がただ 1 つ存在する．

（2） g, l を異なる 2 直線とし，p を l 上にない g の点とする．補題 3.2 より p を通る直線は $n+1$ 個である．一方 $\lambda=1$ で l は $n+1$ 個の点を含むから，p を通り l と共有点をもつ直線は $n+1$ 個存在し，したがってそれらは p を通る直線のすべてである．すなわち g と l はただ 1 点を共有する．

（3） g, l を異なる直線，p_1 を g と l の交点，p_2 を p_1 と異なる g の点，p_3 を p_1 と異なる l の点，p_2, p_3 を通る直線を h とする．このとき g, h, l はすべて異なる直線である．したがって g, l または h 上にある点は $3(n-1)+3=3n$ 個である．一方 $|\Omega|=n^2+n+1$ であるから，$n \geqq 2$ より $n^2+n+1-3n=n^2-2n+1=(n-1)^2 \gneqq 0$ である．したがって，g, l, h のいずれにも含まれない点 p_4 が存在し，4 点 p_1, p_2, p_3, p_4 はいずれの 3 点も同一直線上にない．

以上より 2-$(n^2+n+1, n+1, 1)$ デザイン $(n \geqq 2)$ は射影平面である．□

つぎの 3 条件をみたす結合構造 $(\Omega, \mathfrak{B})$ を**アフィン平面** (affine plane) という．ここでブロックを直線という．

（1） 異なる 2 点を通る直線がただ 1 つ存在する．

（2） 直線 l と l 上にない点 p に対して，p を通り l と共有点をもたない直線がただ 1 つ存在する．

（3） 1直線上にない3点が存在する．

アフィン平面の2直線 l_1, l_2 が $l_1 = l_2$ であるか，共有点をもたないとき l_1 と l_2 は平行であるといい，$l_1 /\!/ l_2$ と書く．つぎの 注 のように平行の関係は同値律をみたし，したがってその同値類を **平行線類** という．なお 2 直線が平行でないとき，2直線は交わるといい，その共有点を2直線の交点という．

注 3.4 アフィン平面において直線の平行の関係は同値律をみたす．

［証 明］ いま l_1, l_2, l_3 をアフィン平面の直線とする．

反射律： $l_1 /\!/ l_1$,

対称律： $l_1 /\!/ l_2 \Rightarrow l_2 /\!/ l_1$

が成り立つことは平行の定義より明らかである．

推移律： $l_1 /\!/ l_2,\ l_2 /\!/ l_3 \Rightarrow l_1 /\!/ l_3$

が成り立つことを示す．l_1 と l_3 が交わらなければ定義より $l_1 /\!/ l_3$ である．いま l_1 と l_3 が交点 p をもつとする．p が l_2 上にあれば，$l_1 /\!/ l_2$ より $l_1 = l_2$, $l_2 /\!/ l_3$ より $l_2 = l_3$ となり $l_1 = l_3$，すなわち $l_1 /\!/ l_3$ である．$p \notin l_2$ とすると，l_1, l_3 は共に p を通り l_2 に平行な直線であるから，アフィン平面の条件（2）より $l_1 = l_3$ となり，$l_1 /\!/ l_3$ である．□

補 題 3.5 2-$(n^2, n, 1)$ デザインにおいて，ブロックの個数は $n^2 + n$ 個，1点を通るブロックの個数は $n + 1$ 個である．

［証 明］ 定理2.8よりブロックの個数は

$$r_0 = 1 \cdot \frac{n^2(n^2-1)}{n(n-1)} = n^2 + n$$

であり，1点を通るブロックの個数は

$$r_1 = 1 \cdot \frac{n^2-1}{n-1} = n + 1$$

である．□

定 理 3.6 結合構造 $(\Omega, \mathfrak{B})$ がアフィン平面であることと，2-$(n^2, n, 1)$ デザイン $(n \geqq 2)$ であることとは同じである．

［証 明］ 定理3.3の証明とほとんど同じである．

（i） $(\Omega, \mathfrak{B})$ をアフィン平面，l を $\mathfrak{B}$ の直線，l 上の点の個数を n とする．アフィン平面の条件（3）より l 上にない任意の点 p をとる．p を通る直線の個数は条件（1）より l と1点で交わる n 個と，条件（2）より l と平行な直線の $n+1$ 個である．

g を l と交わる直線とする．点 p を l 上にも g 上にもない点としてとることができる．なぜならば l と異なり l と平行な直線 l' が条件 (2), (3) より存在する．同様にして g

と異なり g と平行な直線 g' が存在する．l と g は交わるから l' と g' は交わりその交点を p とすればよい．このとき上で示したことより，p を通る直線の個数は $n+1$ 個で，g と平行な1個の直線と，g とただ1点で交わる n 個の直線よりなり，したがって g は n 個の点を含む．つぎに l' を l に平行な任意の直線とすると，l' は g と交わるから l' も n 個の点を含む．以上より任意の直線は n 個の点を含む．

任意の2点を通る直線は条件（1）よりただ1つ存在するから，$(\Omega, \mathfrak{B})$ は会合数 $\lambda=1$ の 2-デザインである．

点 p を通る直線は $n+1$ 個存在し，各直線は n 個の点を含む．条件（1）より p 以外の Ω の点は p を通るちょうど1つの直線に含まれる．したがって Ω の点の個数は $(n-1)(n+1)+1=n^2$ である．また条件（3）より $n \geqq 2$ である．

以上よりアフィン平面は 2-$(n^2, n, 1)$ デザイン $(n \geqq 2)$ である．

(ii) $(\Omega, \mathfrak{B})$ を 2-$(n^2, n, 1)$ デザイン $(n \geqq 2)$ とし，$\mathfrak{B}$ のブロックを直線とよぶことにする．

（1） 会合数 $\lambda=1$ の 2-デザインだから，2点を通る直線がただ1つ存在する．

（2） 直線 l と，l 上にない点 p をとる．補題 3.5 より p を通る直線の個数は $n+1$ 個である．一方 $\lambda=1$ で，l は n 個の点を含むから，p を通り l と交わる直線は n 個である．したがって p を通り l に平行な直線がただ1つ存在する．

（3） 直線 l 上の点の個数は n 個，Ω の点の個数は n^2 個で，$n \geqq 2$ より l 上にない点が存在し l 上の2点とあわせて3点は条件（3）をみたす．

以上より 2-$(n^2, n, 1)$ デザインはアフィン平面である．□

注 3.7 2-$(n^2, n, 1)$ デザインの平行線類はちょうど n 個の平行線を含む．

［証 明］ L を1つの平行線類，g を L に含まれない直線とする．L の各直線は g とちょうど1点で交わり，g 上の各点に対してその点を通る L の直線がちょうど1つ存在する．したがって L に含まれる直線の個数は g 上の点の個数 n に等しい．□

2-$(n^2+n+1, n+1, 1)$ デザインを**位数** n の射影平面，2-$(n^2, n, 1)$ デザインを**位数** n のアフィン平面という．

B_0 を結合構造 $D=(\Omega, \mathfrak{B})$ の1つのブロックとする．$\bar{\Omega}=\Omega-B_0$，$\bar{\mathfrak{B}}=\{\bar{B}=B\cap\bar{\Omega} \mid B\in\mathfrak{B}-\{B_0\}\}$ とするとき結合構造 $\bar{D}=(\bar{\Omega}, \bar{\mathfrak{B}})$ を D の B_0 に関する**外部構造**という．

定 理 3.8 結合構造 $D=(\Omega, \mathfrak{B})$ を位数 n の射影平面，l を D の直線と

するとき，Dの直線lに関する外部構造 $\bar{D}=(\bar{\Omega},\ \bar{\mathfrak{B}})$ は位数nのアフィン平面である．

逆に位数nのアフィン平面は位数nのある射影平面の直線に関する外部構造である．

［証 明］ $D=(\Omega,\mathfrak{B})$ を位数nの射影平面，$l\in\mathfrak{B}$，l に関するDの外部構造を $\bar{D}=(\bar{\Omega},\bar{\mathfrak{B}})$ とする．定理 3.3 より $|\Omega|=n^2+n+1$, $|l|=n+1$ であるから $|\bar{\Omega}|=|\Omega-l|=n^2$ である．gをlと異なる任意の直線とするとgとlはただ1点を共有するから，$|g\cap\bar{\Omega}|=n$ である．p, q を$\bar{\Omega}$の異なる任意の2点とすると，p, q を通る$\mathfrak{B}$の直線がただ1つ存在し，lと異なるからp, qを通る直線もただ1つ存在する．

以上より $\bar{D}=(\bar{\Omega},\bar{\mathfrak{B}})$ は 2-$(n^2, n, 1)$ デザインになり，定理 3.6 より位数nのアフィン平面である．

逆に $\bar{D}=(\bar{\Omega},\bar{\mathfrak{B}})$ を位数nのアフィン平面とすると，補題3.5より$|\bar{\mathfrak{B}}|=n^2+n$ である．また注 3.7 より1つの平行線類はn個の平行線よりなるから，$\bar{\mathfrak{B}}$ に $n+1$ 個の平行線類が存在し，これを $L_1, L_2, \cdots, L_{n+1}$ とする．いま $\bar{\Omega}$ に $p+1$ 個の点 $p_1, p_2, \cdots, p_{n+1}$ を加えて $\Omega=\bar{\Omega}\cup\{p_1, p_2, \cdots, p_{n+1}\}$ とおく．さらに$\bar{\mathfrak{B}}$の直線 $\bar{l}$ に対して，$\bar{l}$ の属する平行線類を L_i とするとき直線 $l=\bar{l}\cup\{p_i\}$ とおく．さらに直線 $l_\infty=\{p_1, p_2, \cdots, p_{n+1}\}$ とおき，$\mathfrak{B}=\{l\mid\bar{l}\in\bar{\mathfrak{B}}\}\cup\{l_\infty\}$ として結合構造 $D=(\Omega,\mathfrak{B})$ を作る．このとき $|\Omega|=|\bar{\Omega}\cup\{p_1, p_2, \cdots, p_{n+1}\}|=n^2+n+1$ であり，$\bar{\mathfrak{B}}$ の各直線はn個の点を含むから$\bar{\mathfrak{B}}$から作られた$\mathfrak{B}$の直線および直線 l_∞ はともに $n+1$ 個の点を含む．

いま任意の $p, q(\neq)\in\Omega$ をとる．$p, q\in\bar{\Omega}$ のとき p, q を通る$\bar{\mathfrak{B}}$の直線はただ1つだから，$\mathfrak{B}$の直線もただ1つである．$p=p_i, q\in\bar{\Omega}$ のとき p_i を通る直線は $\{\bar{l}\cup\{p_i\}\mid\bar{l}\in L_i\}\cup\{l_\infty\}$ の直線に限り，qを通るL_iの直線はただ1つだから，p_i, q を通る$\mathfrak{B}$の直線はただ1つである．$p=p_i, q=p_j$ のとき，この2点を通る$\mathfrak{B}$の直線は l_∞ のみである．

以上より $D=(\Omega,\ \mathfrak{B})$ は 2-$(n^2+n+1, n+1, 1)$ デザインになり，位数nの射影平面である．このときDの作り方より $\bar{D}$ は l_∞ に関するDの外部構造である．□

定 理 3.9 結合構造 $D=(\Omega,\mathfrak{B})$を有限体 $GF(q)$ 上の射影平面 $PG(2, q)$ とすると，$\mathrm{Aut}\,D=P\Gamma L(3, q)$ である．

［証 明］ ベクトル空間 $V=V(3,\ q)$ とし，$D=PG(2,\ q)$ の点を $[v]$ $(v\in V)$ と書く．また以下の証明で $v\in V$ に対して λv と書いたときのvの係数λは $GF(q)$ の元であり，$[v], [v'](\neq)$ に対して，Dの直線 $[\langle v, v'\rangle]$ を単に $[v, v']$ と書く．

$P\Gamma L(3,\ q)$ はΩ上の置換群である．任意の直線 $l=[v_1,\ v_2]$，および任意の $[\sigma_\theta]$

$\in P\Gamma L(3,q)$ ($\sigma_\theta \in \Gamma L(3,q), \theta \in \mathrm{Aut}\,GF(q)$) をとる．任意の $[\alpha v_1 + \beta v_2] \in l$ に対して

$$[\alpha v_1 + \beta v_2]^{[\sigma_\theta]} = [\alpha^\theta v_1{}^{\sigma_\theta} + \beta^\theta v_2{}^{\sigma_\theta}] \in [v_1{}^{\sigma_\theta}, v_2{}^{\sigma_\theta}]$$

であるから，$l^{[\sigma_\theta]}$ は直線 $[v_1{}^{\sigma_\theta}, v_2{}^{\sigma_\theta}]$ となる．すなわち $[\sigma_\theta] \in \mathrm{Aut}\,D$ で $P\Gamma L(3,q) \leqq \mathrm{Aut}\,D$ である．

逆に $\sigma \in \mathrm{Aut}\,D$ とする．$[v], [v'] (\neq) \in D$ に対して $[v]^\sigma = [u]$，$[v']^\sigma = [u']$ とすると，明らかに $[u] \neq [u']$ である．ここで直線 $[v, v']$ 上の $[v']$ と異なる点は $[v + \lambda v']$ と表され，$[u], [u'] \in [v, v']^\sigma$ であるから，$[v, v']^\sigma = [u, u']$，$[v + \lambda v']^\sigma = [u + \lambda' u']$ である．

以下 $\{v_1, v_2, v_3\}$ をVの基とし，$\sigma \in P\Gamma L(3, q)$ を（i）から（iv）にわけて証明する．

（i） つぎをみたすVの基 $\{u_1, u_2, u_3\}$ が存在する．

$$[v_i]^\sigma = [u_i], \qquad [v_i + v_j]^\sigma = [u_i + u_j] \qquad (i, j = 1, 2, 3),$$
$$[v_1 + v_2 + v_3]^\sigma = [u_1 + u_2 + u_3].$$

（証明） $[v_1]^\sigma = [u_1]$ とおき，$[v_2]^\sigma = [u_2']$，$[v_3]^\sigma = [u_3']$ とする．$[v_1 + v_i] \in [v_1, v_i]$ $(i = 2, 3)$ より，$[v_1 + v_i]^\sigma \in [v_1, v_i]^\sigma = [u_1, u_i']$ となり $[v_1 + v_i]^\sigma = [u_1 + \lambda_i u_i']$ $(\lambda_i \neq 0)$ である．いま $\lambda_2 u_2' = u_2$，$\lambda_3 u_3' = u_3$ とおく．

このとき $[v_i]^\sigma = [u_i]$ $(i = 1, 2, 3)$, $[v_1 + v_i]^\sigma = [u_1 + u_i]$ $(i = 2, 3)$ である．ここで $u_3 \in \langle u_1, u_2 \rangle$ であれば $[u_3] \in [u_1, u_2]$，$[u_3]^{\sigma^{-1}} \in [u_1, u_2]^{\sigma^{-1}}$ すなわち $[v_3] \in [v_1, v_2]$ となり $\{v_1, v_2, v_3\}$ が Vの基であることに反する．したがって $\{u_1, u_2, u_3\}$ はVの基である．

$$[v_1 + v_2 + v_3] = [v_1 + v_2, v_3] \cap [v_1 + v_3, v_2]$$

より

$$\begin{aligned}[v_1 + v_2 + v_3]^\sigma &= [v_1 + v_2, v_3]^\sigma \cap [v_1 + v_3, v_2]^\sigma = [u_1 + u_2, u_3] \cap [u_1 + u_3, u_2] \\ &= [u_1 + u_2 + u_3]\end{aligned}$$

である．つぎに $[v_2, v_3]^\sigma = [u_2, u_3]$ より $[v_2 + v_3]^\sigma = [u_2 + \lambda u_3]$ である．一方

$$[v_1 + v_2 + v_3] = [v_1 + v_2, v_3] \cap [v_2 + v_3, v_1]$$

より

$$\begin{aligned}[u_1 + u_2 + u_3] &= [v_1 + v_2 + v_3]^\sigma = [v_1 + v_2, v_3]^\sigma \cap [v_2 + v_3, v_1]^\sigma \\ &= [u_1 + u_2, u_3] \cap [u_2 + \lambda u_3, u_1] = [u_1 + u_2 + \lambda u_3]\end{aligned}$$

となり $\lambda = 1$ すなわち$[v_2 + v_3]^\sigma = [u_1 + u_3]$ である．

（ii） 任意の $\lambda \in GF(q)$ に対して $[v_1+\lambda v_2]^\sigma = [u_1+\bar{\lambda} u_2]$ とするとき，写像 θ: $GF(q) \to GF(q)$, $\lambda \mapsto \bar{\lambda}$ は全単射で $1^\theta = 1$ である．

（証明） $[v_1, v_2]^\sigma = [u_1, u_2]$ であるから，任意の $\lambda \in GF(q)$ に対して $[v_1+\lambda v_2]^\sigma = [u_1+\bar{\lambda} u_2]$ である．ここで $\bar{\lambda}$ は λ により一意的に決まるから，写像 $\theta: GF(q) \to GF(q)$ が $\lambda \mapsto \bar{\lambda}$ により定義できる．このとき $[v_1+v_2]^\sigma = [u_1+u_2]$ で一方 $[v_1+v_2]^\sigma = [v_1+1\cdot v_2]^\sigma = [u_1+1^\theta\cdot u_2]$ であるから，$1^\theta = 1$ である．また $\lambda \neq \lambda'$ のとき $[v_1+\lambda v_2] \neq [v_1+\lambda' v_2]$ だから $[v_1+\lambda v_2]^\sigma \neq [v_1+\lambda' v_2]^\sigma$ すなわち $[u_1+\lambda^\theta u_2] \neq [u_1+\lambda'^\theta u_2]$ となり，$\lambda^\theta \neq \lambda'^\theta$ である．したがって θ は単射になり，さらに $GF(q)$ は有限集合だから θ は全射である．

（iii） $[v_i+\lambda v_j]^\sigma = [u_i+\lambda^\theta u_j]$ （$\{i, j\} = \{2, 3\}$），$[v_1+\lambda v_2+\mu v_3]^\sigma = [u_1+\lambda^\theta u_2 + \mu^\theta u_3]$ である．

（証明）
$$[v_1, v_2+v_3]^\sigma = [u_1, u_2+u_3]$$
より
$$[v_1+\lambda(v_2+v_3)]^\sigma = [u_1+\lambda'(u_2+u_3)]$$
である．一方
$$[v_1+\lambda v_2] = [v_1, v_2] \cap [v_3, v_1+\lambda(v_2+v_3)]$$
より
$$\begin{aligned}[u_1+\lambda^\theta u_2] &= [v_1+\lambda v_2]^\sigma = [v_1, v_2]^\sigma \cap [v_3, v_1+\lambda(v_2+v_3)]^\sigma \\ &= [u_1, u_2] \cap [u_3, u_1+\lambda'(u_2+u_3)] = [u_1+\lambda' u_2]\end{aligned}$$
となり $\lambda' = \lambda^\theta$ である．したがって
$$[v_1+\lambda v_3] = [v_1, v_3] \cap [v_2, v_1+\lambda(v_2+v_3)]$$
より
$$\begin{aligned}[v_1+\lambda v_3]^\sigma &= [v_1, v_3]^\sigma \cap [v_2, v_1+\lambda(v_2+v_3)]^\sigma \\ &= [u_1, u_3] \cap [u_2, u_1+\lambda^\theta(u_2+u_3)] = [u_1+\lambda^\theta u_3]\end{aligned}$$
である．つぎに $\{i, j\} = \{2, 3\}$ とすると
$$[v_i+\lambda v_j]^\sigma = [u_i+\lambda'' u_j]$$
である．ここで
$$[v_1+v_i+\lambda v_j] = [v_1, v_i+\lambda v_j] \cap [v_j, v_1+v_i]$$
より
$$\begin{aligned}[v_1+v_i+\lambda v_j]^\sigma &= [v_1, v_i+\lambda v_j]^\sigma \cap [v_j, v_1+v_i]^\sigma \\ &= [u_1, u_i+\lambda'' u_j] \cap [u_j, u_1+u_i] = [u_1+u_i+\lambda'' u_j]\end{aligned}$$

である．一方

$$[v_1 + v_i + \lambda v_j] = [v_i, v_1 + \lambda v_j] \cap [v_j, v_1 + v_i]$$

より

$$[v_1 + v_i + \lambda v_j]^\sigma = [v_i, v_1 + \lambda v_j]^\sigma \cap [v_j, v_1 + v_i]^\sigma$$
$$= [u_i, u_1 + \lambda^\theta u_j] \cap [u_j, u_1 + u_i] = [u_1 + u_i + \lambda^\theta u_j]$$

である．したがって $\lambda'' = \lambda^\theta$ となり

$$[v_i + \lambda v_j]^\sigma = [u_i + \lambda^\theta u_j] \qquad (\{i, j\} = \{2, 3\})$$

である．さらに

$$[v_1 + \lambda v_2 + \mu v_3] = [v_1 + \lambda v_2, v_3] \cap [v_1 + \mu v_3, v_2]$$

より

$$[v_1 + \lambda v_2 + \mu v_3]^\sigma = [v_1 + \lambda v_2, v_3]^\sigma \cap [v_1 + \mu v_3, v_2]^\sigma$$
$$= [u_1 + \lambda^\theta u_2, u_3] \cap [u_1 + \mu^\theta u_3, u_2] = [u_1 + \lambda^\theta u_2 + \mu^\theta u_3]$$

が成り立つ．

（iv） $\theta \in \mathrm{Aut}\, GF(q)$ である．

（証明） $$[v_1 + \lambda\mu v_2 + \mu v_3] = [v_1, \lambda v_2 + v_3] \cap [v_2, v_1 + \mu v_3]$$

より

$$[v_1 + \lambda\mu v_2 + \mu v_3]^\sigma = [v_1, \lambda v_2 + v_3]^\sigma \cap [v_2, v_1 + \mu v_3]^\sigma$$
$$[u_1 + (\lambda\mu)^\theta u_2 + \mu^\theta u_3] = [u_1, \lambda^\theta u_2 + u_3] \cap [u_2, u_1 + \mu^\theta u_3]$$
$$= [u_1 + \lambda^\theta \mu^\theta u_2 + \mu^\theta u_3]$$

となり，$(\lambda\mu)^\theta = \lambda^\theta \mu^\theta$ である．つぎに

$$[v_1 + (\lambda + \mu) v_2 + v_3] = [v_1 + \lambda v_2, v_3 + \mu v_2] \cap [v_1 + v_3, v_2]$$

より

$$[v_1 + (\lambda + \mu) v_2 + v_3]^\sigma = [v_1 + \lambda v_2, v_3 + \mu v_2]^\sigma \cap [v_1 + v_3, v_2]^\sigma$$
$$[u_1 + (\lambda + \mu)^\theta u_2 + u_3] = [u_1 + \lambda^\theta u_2, u_3 + \mu^\theta u_2] \cap [u_1 + u_3, u_2]$$
$$= [u_1 + (\lambda^\theta + \mu^\theta) u_2 + u_3]$$

となり，$(\lambda + \mu)^\theta = \lambda^\theta + \mu^\theta$ である．したがって θ は（ii）より $GF(q)$ の自己同型である．

（v） $[\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3]^\sigma = [\lambda_1{}^\theta u_1 + \lambda_2{}^\theta u_2 + \lambda_3{}^\theta u_3]$ である．

（証明） $\lambda_1 \neq 0$ とするとき，$\theta \in \mathrm{Aut}\, GF(q)$ より（iii）を用いて

$$[\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3]^\sigma = [v_1 + \lambda_1{}^{-1}\lambda_2 v_2 + \lambda_1{}^{-1}\lambda_3 v_3]^\sigma$$
$$= [u_1 + (\lambda_1{}^\theta)^{-1}\lambda_2{}^\theta u_2 + (\lambda_1{}^\theta)^{-1}\lambda_3{}^\theta u_3] = [\lambda_1{}^\theta u_1 + \lambda_2{}^\theta u_2 + \lambda_3{}^\theta u_3]$$

である．$\lambda_1=0$ のとき $\lambda_2\neq 0$ または $\lambda_3\neq 0$ だから，$\lambda_2\neq 0$ としてよい．このとき同様に (iii) を用いて

$$[\lambda_1 v_1+\lambda_2 v_2+\lambda_3 v_3]^\sigma=[\lambda_2 v_2+\lambda_3 v_3]^\sigma=[v_2+\lambda_2^{-1}\lambda_3 v_3]^\sigma=[u_2+(\lambda_2^\theta)^{-1}\lambda_3^\theta u_3]$$
$$=[\lambda_2^\theta u_2+\lambda_3^\theta u_3]=[\lambda_1^\theta u_1+\lambda_2^\theta u_2+\lambda_3^\theta u_3]$$

となり任意の $\lambda_1,\lambda_2,\lambda_3$ に対して (v) の式が成り立つ．

(vi) $\mathrm{Aut}\,D=P\Gamma L(3,q)$ である．

(証明) $\{v_1,v_2,v_3\}$，$\{u_1,u_2,u_3\}$ はVの基で，$\theta\in\mathrm{Aut}\,GF(q)$ であるから，写像 φ: $V\to V$ を $(\sum_{i=1}^{3}\lambda_i v_i)^\varphi=\sum_{i=1}^{3}\lambda_i^\theta u_i$ により定義するとφは $\Gamma L(3,q)$ の元である．このとき $[\varphi]\in P\Gamma L(3,q)$ となり (v) より $[\varphi]$ と σは一致する．すなわち $\sigma\in P\Gamma L(3,q)$ となり $\mathrm{Aut}\,D=P\Gamma L(3,q)$ である．□

注 3.10 結合構造 $D=(\Omega,\mathfrak{B})$ を有限体 $GF(q)$ 上の射影平面 $PG(2,q)$ とする．このとき直線 l に関するDの外部構造は直線 l のとり方に関係なく同型である．これを **$GF(q)$ 上のアフィン平面**といい，$AG(2,q)$ と書く．

［証明］ l,g を $PG(2,q)$ の任意の直線とし，$l=[\langle v_1,v_2\rangle]$，$g=[\langle u_1,u_2\rangle]$ $(v_1,v_2,u_1,u_2\in V(3,q))$ とする．定理 2;10.5 より $P\Gamma L(3,q)$は Ω上2重可移だから，$[\sigma]\in P\Gamma L(3,q)$が存在して，$[v_1]^{[\sigma]}=[u_1]$，$[v_2]^{[\sigma]}=[u_2]$ で，したがって $l^{[\sigma]}=g$ である．$\overline{D^{(1)}}$，$\overline{D^{(2)}}$ をそれぞれ l,g に関するDの外部構造とすると，$[\sigma]\in\mathrm{Aut}\,D$ だから $[\sigma]$ は $\overline{D^{(1)}}$ から$\overline{D^{(2)}}$ の上への同型写像を導く．□

定理 3.11 $D^{(1)}=(\Omega^{(1)},\mathfrak{B}^{(1)})$，$D^{(2)}=(\Omega^{(2)},\mathfrak{B}^{(2)})$を共に射影平面，$\overline{D^{(1)}}=(\overline{\Omega^{(1)}},\overline{\mathfrak{B}^{(1)}})$，$\overline{D^{(2)}}=(\overline{\Omega^{(2)}},\overline{\mathfrak{B}^{(2)}})$ を共にアフィン平面とする．いま $\overline{D^{(1)}}$，$\overline{D^{(2)}}$ がそれぞれ $D^{(1)},D^{(2)}$ のある直線に関する外部構造で，$\overline{D^{(1)}}$，$\overline{D^{(2)}}$ が同型であれば $D^{(1)}$ と $D^{(2)}$ も同型である．

［証明］ $\overline{D^{(1)}}$，$\overline{D^{(2)}}$ をそれぞれ $D^{(1)}$，$D^{(2)}$ の直線 $l^{(1)}$，$l^{(2)}$ に関する外部構造，$\overline{D^{(1)}}$ の平行線類を $L_1^{(1)}$，$L_2^{(1)}$，…，$L_{n+1}^{(1)}$，$\overline{D^{(1)}}$ から $\overline{D^{(2)}}$ への同型写像を $\bar{f}$ とする．$L_i^{(1)}$ に含まれる平行線の $\bar{f}$ による像の集まりを $L_i^{(2)}$ とすると，$\overline{D^{(2)}}$ の平行線類は $L_1^{(2)}$，$L_2^{(2)}$，…，$L_{n+1}^{(2)}$ である．平行線類 $L_i^{(1)}$ によって定まる $l^{(1)}$ の点を p_i すなわちすべての $\bar{l}\in L_i^{(1)}$ に対して $\bar{l}\cup\{p_i\}$ が $D^{(1)}$ の直線になる点を p_i とし，同様に平行線類 $L_i^{(2)}$ によって定まる $l^{(2)}$ の点を q_i $(i=1,2,\cdots,n+1)$ とする．

$\Omega^{(1)}$ から $\Omega^{(2)}$ への写像fをつぎのように定義する．$\overline{\Omega^{(1)}}$ の点pに対しては $p^f=p^{\bar{f}}$ とし，$l^{(1)}$ の点 p_i に対しては $p_i^f=q_i$ $(i=1,2,\cdots,n+1)$ とする．このときfは $\Omega^{(1)}$

から $\Omega^{(2)}$ への全単射である．また $\mathfrak{B}^{(1)}$ の直線 $l = \dot{l} \cup \{p_i\}$, $l \in L_i^{(1)}$, に対しては $l^f = \dot{l}^f \cup \{q_i\} \in \mathfrak{B}^{(2)}$ となり，$l^{(1)}$ に対しては $(l^{(1)})^f = l^{(2)}$ である．したがって $(\mathfrak{B}^{(1)})^f = \mathfrak{B}^{(2)}$ となり，f は $D^{(1)}$ から $D^{(2)}$ への同型である．すなわち $D^{(1)}$ と $D^{(2)}$ は同型である．□

定 理 3.12 結合構造 $D = (\Omega, \mathfrak{B})$ を射影平面 $PG(2, q)$, D の直線 l に関する外部構造を $\bar{D} = (\bar{\Omega}, \bar{\mathfrak{B}})$ とし，$G = \mathrm{Aut}\, D$, $\bar{G} = \mathrm{Aut}\, \bar{D}$ とおく．このとき $G = P\Gamma L(3, q)$ で，$\bar{D}$ はアフィン平面 $AG(2, q)$ であるがさらに$\bar{G}$についてつぎのことが成り立つ．

（1） $\bar{G} = G^{\bar{\Omega}}$ で $\bar{G}$ はGにおける直線 l 上の点の集合としての安定化群 $G_{(l)}$ に同型である，すなわち $\bar{G} = G^{\bar{\Omega}} \cong G_{(l)}$ である．

（2） Gにおける直線 l 上のすべての点の安定化群を G_l, $(G_l)^{\bar{\Omega}} = L$ とおくと，$\bar{G}/L \cong G^l \cong P\Gamma L(2, q)$ である．

（3） Lは $\bar{\Omega}$ 上 Frobenius 群で，Nを L の Frobenius 核，Hを L の Frobenius 補群とする．このときNは加法群としての $GF(q)$ の直積 $GF(q) \times GF(q)$ に同型でしたがって基本可換群である．また $H \cong L/N$ は乗法群としての $GF(q)^\#$ に同型である．

（4） $|\bar{G}| = |P\Gamma L(3, q)|/(q^2 + q + 1) = |P\Gamma L(2, q)| \cdot q^2(q-1)$ で $\bar{G}$ は $\bar{\Omega}$ 上 2 重可移である．

［証 明］ ベクトル空間$V = V(3, q)$ のベクトルvによりDの点を $[v]$, $\sigma \in \Gamma L(3, q)$ により $P\Gamma L(3, q)$ の元を $[\sigma]$ とし，Dの 2 点 $[v], [v']$ を通る直線を $[v, v']$ と書く．また λv と書いたときのベクトルvの係数 λ はすべて $GF(q)$ の元とする．定理 3.9 より $G = P\Gamma L(3, q)$ である．

（1） $G^{\bar{\Omega}} = (G_{(l)})^{\bar{\Omega}} \cong G_{(l)}/(G_{(l)})_{\bar{\Omega}}$ である．ここで $(G_{(l)})_{\bar{\Omega}}$ は$\bar{\mathfrak{B}}$のすべての平行線類を固定し，したがって l のすべての点を固定する．すなわち $(G_{(l)})_{\bar{\Omega}} = 1$ となり，$G^{\bar{\Omega}} \cong G_{(l)}$ である．

$[\sigma] \in G_{(l)}$ に対して $[\sigma]^{\bar{\Omega}} = \overline{[\sigma]}$と書く．任意の $l \in \bar{\mathfrak{B}}$ に対して $[v] \in l$ が存在して $l \cup \{[v]\} \in \mathfrak{B}$である．よって任意の $[\sigma] \in G_{(l)}$ に対して，$(l \cup \{[v]\})^{[\sigma]} = l^{\overline{[\sigma]}} \cup \{[v]^{[\sigma]}\}$, $[v]^{[\sigma]} \in l$ であるから，$l^{\overline{[\sigma]}} \in \bar{\mathfrak{B}}$ となる．すなわち $\bar{\mathfrak{B}}^{\overline{[\sigma]}} = \bar{\mathfrak{B}}$ で，これより $G^{\bar{\Omega}} \leqq \bar{G}$ である．

逆に $\bar{\sigma} \in \bar{G}$ は定理 3.11 の証明におけるように，直線 l を固定するDの自己同型$[\sigma]$

に拡張される．したがって $G^{\bar{\Omega}}=\bar{G}$ である．

（2） $l=[v_1, v_2]$ とする．任意の $[\sigma_\theta]\in G_{(l)}$ $(\theta\in \mathrm{Aut}\,GF(q))$，任意の $[\lambda_1 v_1+\lambda_2 v_2]\in l$ に対して $[\lambda_1 v_1+\lambda_2 v_2]^{[\sigma_\theta]}=[\lambda_1{}^\theta v_1{}^{\sigma_\theta}+\lambda^\theta{}_2 v_2{}^{\sigma_\theta}]\in l$ であるから，$[\sigma_\theta]$ は l 上 $P\Gamma L(2,q)$ の元である．

逆に l 上の $\Gamma L(2,q)$ の元 $\sigma_\theta{}'$ をとり，$v_1{}^{\sigma_\theta{}'}=u_1$，$v_2{}^{\sigma_\theta{}'}=u_2$ とする．いま l 上にない Ω の点 $[v_3]$ をとると，$\{v_1, v_2, v_3\}$ および $\{u_1, u_2, u_3=v_3\}$ は V の基である．したがって任意の $\sum_{i=1}^{3}\lambda_i v_i\in V$ に対して $(\sum_{i=1}^{3}\lambda_i v_i)^{\sigma_\theta}=\sum_{i=1}^{3}\lambda_i{}^\theta u_i$ により V 上の写像 σ_θ を定義すると，$[\sigma_\theta]\in P\Gamma L(3,q)$ で $[\sigma_\theta]$ は l 上 $[\sigma_\theta{}']$ に一致する．

以上より $G^l\cong P\Gamma L(2,q)$ であり，$G^l\cong G_{(l)}/G_l$ である．ここで $G_{(l)}\cong\bar{G}$ において $G_{(l)}$ の部分群 G_l に対応する $\bar{G}$ の部分群は $\bar{G}=G^{\bar{\Omega}}$ より $(G_l)^{\bar{\Omega}}=L$ である．したがって $G_{(l)}/G_l\cong\bar{G}/L$ となり $\bar{G}/L\cong P\Gamma L(2,q)$ である．

（3） $l=[v_1, v_2]$ とし，$[v_3]\notin l$ をとると $\{v_1, v_2, v_3\}$ はVの基である．

$$\tau(\alpha,\beta)=\begin{pmatrix}1&0&0\\0&1&0\\\alpha&\beta&1\end{pmatrix}$$

とおくと；$\tau(\alpha,\beta)\in GL(V)$ であり，$N=\{[\tau(\alpha,\beta)]\,|\,\alpha,\beta\in GF(q)\}$ とおく．また $v\in V$ の基 $\{v_1, v_2, v_3\}$ に関する座標を $v=(\lambda_1,\lambda_2,\lambda_3)$，$[v]=[\lambda_1,\lambda_2,\lambda_3]$ とすると

$$[\lambda_1,\lambda_2,\lambda_3]^{[\tau(\alpha,\beta)]}=[\lambda_1+\alpha\lambda_3, \lambda_2+\beta\lambda_3, \lambda_3]$$

である．したがって任意の l 上の点 $[\lambda_1,\lambda_2,0]$ に対して

$$[\lambda_1,\lambda_2,0]^{[\tau(\alpha,\beta)]}=[\lambda_1,\lambda_2,0]$$

となり，$[\tau(\alpha,\beta)]$ は l 上のすべての点を固定する．これより $N\subseteqq G_l$ である．

$\bar{\Omega}$ の任意の点 $[v]=[\lambda_1,\lambda_2,1]$ に対して

$$[\lambda_1,\lambda_2,1]^{[\tau(\alpha,\beta)]}=[\lambda_1+\alpha, \lambda_2+\beta, 1]$$

であるから $[v]^{[\tau(\alpha,\beta)]}=[v]$ となるのは $\alpha=\beta=0$ のときのみである．すなわち単位元 $[\tau(0,0)]$ 以外のNの元は $\bar{\Omega}$ 上に固定点をもたない．さらに

$$[\tau(\alpha,\beta)]\cdot[\tau(\alpha',\beta')]=[\tau(\alpha+\alpha',\beta+\beta')]\in N$$

であるから，Nは G_l の部分群である．また α,β のとり方より $|N|=q^2=|\bar{\Omega}|$ となり，Nは $\bar{\Omega}$ 上正則である．

Nから $GF(q)$ の加法群の直積 $GF(q)\times GF(q)$ への写像を $[\tau(\alpha,\beta)]\mapsto(\alpha,\beta)$ により定義すると明らかに同型写像である．したがって $N\cong GF(q)\times GF(q)$（加法群の直積）となり，これよりNは基本可換群になる．

なお Nは l 上のすべての点を固定するから，Nと $N^{\bar{\Omega}}$ を同一視してよい．

いま $[u_1], [u_2]$ を $\bar{\Omega}$ の異なる 2 点とし，$[\sigma] \in G_l$ がこの 2 点を固定するとする．任意の $[v] \in \bar{\Omega} - [u_1, u_2]$ に対して，$[v, u_1] \cap l = [u_1']$, $[v, u_2] \cap l = [u_2']$ とする．このとき $[u_1, u_1']^{[\sigma]} = [u_1, u_1']$, $[u_2, u_2']^{[\sigma]} = [u_2, u_2']$ で $[u_1, u_1'] \cap [u_2, u_2'] = [v]$ であるから，$[\sigma]$ は $[v]$ を固定する．また $[u_1, u_2]$ 上の点に対しては $\bar{\Omega} - [u_1, u_2]$ の任意の点をとることにより，同様に $[\sigma]$ は $[u_1, u_2]$ 上のすべての点を固定し，以上より $[\sigma] = 1$ となる．すなわちLは $\bar{\Omega}$ 上の置換群として Frobenius 群になり，したがってNはLの Frobenius 核になる．

$H = (G_l)_{[v_3]}$ とおき，Hを $\bar{\Omega}$ 上の置換群とみなすとき，Lの Frobenius 補群である．Hは直線 $[v_1, v_3]$ を固定し $[v_1, v_3] - \{[v_1], [v_3]\}$ 上半正則であるから，$|H| \leqq q-1$ である．

$$\sigma(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

とおくと $\sigma(\alpha) \in GL(V)$ である．$[v_1, v_2]$ の任意の点 $[\lambda_1, \lambda_2, 0]$ に対して

$$[\lambda_1, \lambda_2, 0]^{[\sigma(\alpha)]} = [\lambda_1, \lambda_2, 0]$$

であるから $[\sigma(\alpha)] \in G_l$ である．また $[v_1, v_3]$ の任意の点 $[\lambda_1, 0, \lambda_3]$ に対して

$$[\lambda_1, 0, \lambda_3]^{[\sigma(\alpha)]} = [\lambda_1, 0, \alpha\lambda_3]$$

で特に $[v_3]^{[\sigma(\alpha)]} = [v_3]$ である．したがって $[\sigma(\alpha)] \in H$ で位数より $H = \{\sigma(\alpha) \mid \alpha \in GF(q)^*\}$, $|H| = q-1$ となりHは $[v_1, v_3] - \{[v_1], [v_3]\}$ 上正則となる．

H から乗法群 $GF(q)^*$ への写像を $[\sigma(\alpha)] \mapsto \alpha$ により定義すると，$[\sigma(\alpha)] \cdot [\sigma(\beta)] = [\sigma(\alpha\beta)]$ であるから，明らかにこの写像は同型で，Hと乗法群 $GF(q)^*$は同型である．

（4） GはΩ上 2 重可移であるから，Gは$\mathfrak{B}$上可移である．したがって$|\mathfrak{B}| = q^2+q+1$ より $|G_{(l)}| = |G|/(q^2+q+1)$ である．ここで $\bar{G} \cong G_{(l)}$ で $G = P\Gamma L(3, q)$ であるから，$|\bar{G}| = |P\Gamma L(3, q)|/(q^2+q+1)$ である．さらに (3) の$L=NH$を用いて $|\bar{G}| = |G_{(l)}/G_l| \cdot |G_l| = |P\Gamma L(2, q)| \cdot |NH| = |P\Gamma L(2, q)| \cdot q^2(q-1)$ でもある．

つぎに$\bar{G}$が $\bar{\Omega}$ 上 2 重可移を示す．ここで$\bar{G}$は $\bar{\Omega}$ 上可移であるから，$[v_3] \in \bar{\Omega}$ をとり $\bar{G}_{[v_3]}$ が $\bar{\Omega} - \{[v_3]\}$ 上可移であることを示せばよい．任意の 2 点 $[u_1]$, $[u_2] \in \bar{\Omega} - \{[v_3]\}$ をとる．$[u_2] \in [u_1, v_3]$ であれば，(3) より $L_{[v_3]}$ は $[u_1]$ を $[u_2]$ にうつす元をもつ．いま $[u_2] \notin [u_1, v_3]$ とし，$l \cap [u_1, v_3] = [v_1]$, $l \cap [u_2, v_3] = [v_2]$ とする．$[v_1] \neq [v_2]$ であるから $\{v_1, v_2, v_3\}$ はVの基となり，この基に関する $GL(V)$ の元

$$\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

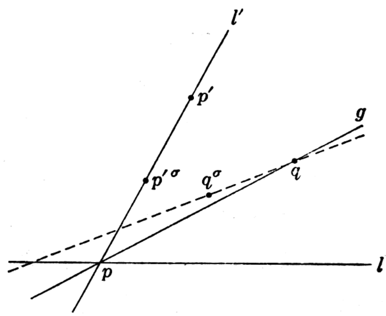
をとる．このとき $[v_1]^{[\sigma]}=[v_2]$，$[v_2]^{[\sigma]}=[v_1]$，$[v_3]^{[\sigma]}=[v_3]$ となり，$l^{[\sigma]}=l$，$[\sigma]\in(G_{(l)})_{[v_3]}$ である．すなわち $[\sigma]^{\bar{\Omega}}\in\bar{G}_{[v_3]}$ である．さらに，$[u_1, v_3]^{[\sigma]}=[v_1, v_3]^{[\sigma]}=[v_2, v_3]=[u_2, v_3]$ となり $[u_1]^{[\sigma]}\in[u_2, v_3]$ である．したがって(3)より $L_{[v_3]}$ は $[u_1]^{[\sigma]}$ を $[u_2]$ にうつす元をもつから $\bar{G}_{[v_3]}$ は $[u_1]$ を $[u_2]$ にうつす元をもつ．以上より $\bar{G}$ は $\bar{\Omega}$ 上２重可移である．□

注 3.13　σ を射影平面 D の自己同型とする．いま σ がある直線 l 上のすべての点を固定するならば，１点 p が存在して，p を通るすべての直線を固定する．

［証 明］　２点 $p_1, p_2(\neq)$ を通る直線を $\overline{p_1p_2}$ と書く．

（ｉ）　σ が l 上にない点 p を固定するとする．g を p を通る任意の直線とし，$l\cap g=q$ とする．このとき $p^\sigma=p$, $q^\sigma=q$ であるから，$g^\sigma=(\overline{pq})^\sigma=\overline{pq}=g$ となる．すなわち σ は p を通る直線をすべて固定する．

（ii）　σ は l 上以外の点は固定しないとする．$p'\notin l$ をとり $l'=\overline{p'p'^\sigma}$, $l\cap l'=p$ とおく．このとき $l'^\sigma=\overline{p'p'^{\sigma\sigma}}=\overline{p'p}^\sigma=\overline{p'^\sigma p}=l'$ となり，σ は l' を固定する．g を p を通り l, l' と異なる任意の直線，q を p と異なる g 上の点とする．l' と同様に σ は直線 $\overline{qq^\sigma}$ を固定し，よって l' と $\overline{qq^\sigma}$ の交点を固定する．ここで σ は l 上以外に固定点をもたないから，$l'\cap\overline{qq^\sigma}=p$ である．すなわち $qq^\sigma=g$ となり σ は g を固定する．ここで g は p を通る任意の直線であるから，σ は p を通るすべての直線を固定する．□



3－1 図

σ を射影平面 D の自己同型とする．D に直線 l と点 p が存在して，σ が l 上のすべての点と，p を通るすべての直線を固定するとき，σ を p を中心とし l を軸とする**配景写像**という．さらに $p\in l$ のとき σ を **elation**，$p\notin l$ のとき σ を **homology** という．

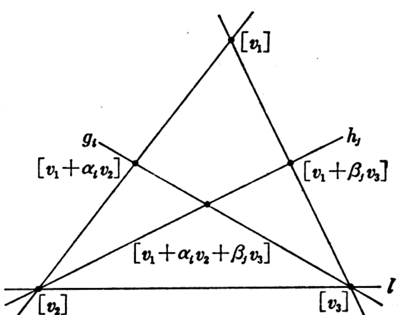
注 3.13 より定理 3.12 における G_l は配景写像よりなり，Frobenius 核 N を導く G_l の部分群は G_l の elation 全体よりなる．したがって G_l の残りの元はすべて homology である．また N をアフィン平面の**平行移動群**（translation group）ともいう．

アフィン平面においてつぎのようにして，点の**座標**が定義される．A を位数 n のアフィン平面，$L_1=\{g_1, g_2, \cdots, g_n\}$, $L_2=\{h_1, h_2, \cdots, h_n\}$ を A の異なる2つの平行線類とする．A の任意の点 p に対して，p を通る L_1 および L_2 の直線がそれぞれただ1つ存在する．いまこの直線を g_i と h_j とするとき，点 p の座標を (i, j) とする．このとき任意の $i, j\in\{1, 2, \cdots, n\}$ に対して座標が (i, j) である点は直線 g_i と直線 h_j の交点としてただ1つ存在するから，A の点と $\{(i, j)\,|\,i, j=1, 2, \cdots, n\}$ は1対1に対応する．

l を射影平面 $PG(2, q)$ の直線とする．ベクトル空間 $V(3, q)$ の基 $\{v_1, v_2, v_3\}$ を $l=[\langle v_2, v_3\rangle]$ にとる．このとき l 上にない $PG(2, q)$ の点のこの基に関する座標は $[1, \lambda, \mu]$ $(\lambda, \mu\in GF(q))$ である．$PG(2, q)$ の直線 l に関する外部構造 $AG(2, q)$ をとる．$AG(2, q)$ の平行線類

$$L_1=\{g_1, g_2, \cdots, g_q\},\qquad L_2=\{h_1, h_2, \cdots, h_q\},\qquad g_i=[\langle v_1+\alpha_i v_2, v_3\rangle],$$
$$h_j=[\langle v_1+\beta_j v_3, v_2\rangle],\qquad \{\alpha_1, \alpha_2, \cdots, \alpha_q\}=\{\beta_1, \beta_2, \cdots, \beta_q\}=GF(q)$$

とする．このとき $AG(2, q)$ の点は g_i と h_j の交点として座標 $[1, \alpha_i, \beta_j]$ をもつ．したがって $[1, \alpha_i, \beta_j]$ と (i, j) を対応させることにより上で述べたアフィン平面の座標がえられる．



3-2 図

A を位数 n のアフィン平面とし，2つの平行線類 $L_1=\{g_1, g_2, \cdots, g_n\}$, $L_2=\{h_1, h_2, \cdots, h_n\}$ により座標 (i, j) を与える．A は $n(n+1)$ 個の直線をもつから，$L_1\cup L_2$ に含まれない直線が $n(n-1)$ 個存在し，それを $l_1, l_2, \cdots, l_{n(n-1)}$ とする．ここで $n(n-1)\times n$ 行列 $M(A)=(a_{ij})$ をつぎのように定義し，アフィン平面 A の行列ということにする．

$a_{ij}\in\{1, 2, \cdots, n\}$ で直線 l_i と直線 g_j との交点の座標が (j, k) のとき $a_{ij}=k$ とする．

このとき $M(A)$ はつぎの性質をもつ．

（1） $l_i=\{(1, a_{i1}), (2, a_{i2}), \cdots, (n, a_{in})\}$ で，$\{a_{i1}, a_{i2}, \cdots, a_{in}\}=\{1, 2, \cdots, n\}$

である．

（2） $i \neq i'$ のとき $a_{ij} = a_{i'j}$ となる j は高々1つである．

(1), (2) が成り立つことはつぎのようにしてわかる．いま $a_{ij} = a_{ij'} = k$ とすると直線 l_i は直線 h_k と (j, k), (j', k) で交わり，したがって $j = j'$ である．これより $j \neq j'$ であれば $a_{ij} \neq a_{ij'}$ となり，$\{a_{i1}, a_{i2}, \cdots, a_{in}\} = \{1, 2, \cdots, n\}$ である．また $i \neq i'$ のとき l_i と $l_{i'}$ は高々1点で交わるから，$a_{ij} = a_{i'j}$ となる j は高々1つである．

逆に $n(n-1) \times n$ 行列よりアフィン平面がつぎのようにして作られる．

定理 3.14 (Witt) $n(n-1) \times n$ 行列 $M = (a_{ij})$, $a_{ij} \in \{1, 2, \cdots, n\}$, $n \geqq 2$ がつぎの性質をもつとする．

（1） $\{a_{i1}, a_{i2}, \cdots, a_{in}\} = \{1, 2, \cdots, n\}$.

（2） $i \neq i'$ のとき $a_{ij} = a_{i'j}$ となる j が高々1つ存在する．

このときつぎの結合構造 A は位数 n のアフィン平面である．

（i） A の点集合は $\Omega = \{(i, j) \mid i, j = 1, 2, \cdots, n\}$ である．

（ii） A の直線は Ω の部分集合 $g_i (i = 1, 2, \cdots, n)$, $h_i (i = 1, 2, \cdots, n)$, l_i $(i = 1, 2, \cdots, n(n-1))$ である．ここで

$$g_i = \{(i, j) \mid j = 1, 2, \cdots, n\},$$
$$h_i = \{(j, i) \mid j = 1, 2, \cdots, n\},$$
$$l_i = \{(j, a_{ij}) \mid j = 1, 2, \cdots, n\}$$

である．

［証 明］ $|\Omega| = n^2$ で各直線は n 個の点を含む．点 (i, j) を通る直線は g_i, h_j および $a_{ki} = j$ である l_k である．したがって異なる2点 (i, j), (i', j') を通る直線は

（a） $i = i'$, $j \neq j'$ のときは g_i のみである．

（b） $i \neq i'$, $j = j'$ のときは h_j のみである．

（c） $i \neq i'$, $j \neq j'$ のとき行列 M において $a_{ki} = j, a_{ki'} = j'$ となる k が存在するとき直線 l_k は (i, j), (i', j') を通り，k が存在しても，条件（2）より l_k のみである．

以上より A の2点を通る直線は高々1つ存在する．したがって各直線は n 個の点を含むから，A は高々 $\binom{n^2}{2} \Big/ \binom{n}{2} = n^2(n^2-1)/n(n-1) = n(n+1)$ 個の直線をもつ．一方 A の直線は g_i, h_i, l_i の $n + n + n(n-1) = n(n+1)$ 個である．すなわち任意の2点を通る直線がただ1つ必ず存在する．

したがってAは 2-$(n^2, n, 1)$ デザインになり，位数nのアフィン平面である．□

補 題 3.15 A, A' を位数nのアフィン平面とし，$M(A)$，$M(A')$ をそれぞれ A, A' の行列とする．いま $M(A')$ が $M(A)$ の行および列を入れかえてえられるならば，Aと A' は同型なアフィン平面である．

［証 明］ $M(A')$ の i 行と j 行の入れかえた行列は，それぞれの行よりできる A' の直線 l_i と l_j の番号 i, j を交換したときにえられる行列である．

また i 列と j 列を入れかえた行列は，A' の座標を定義する直線 g_i と g_j の番号 i, j を交換したときにえられる行列である．

したがって $M(A')$ の行および列の入れかえにそって A' の直線の番号を上に述べたようにうちかえると，Aと A' の同じ番号の直線が対応する同型がえられる．□

定 理 3.16 (Witt) 位数 2, 3, 4 のアフィン平面がただ1つ存在する．

［証 明］ $AG(2,2)$，$AG(2,3)$，$AG(2,4)$ はそれぞれ位数 2, 3, 4 のアフィン平面である．いまMをアフィン平面Aの行列とする．

Aを位数2とする．このときMは 2×2 行列で行列

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

または，この行列の行，列を入れかえたものであるから補題 3.15 より位数2のアフィン平面はすべて同型である．

Aを位数3とする．このときMは 6×3 行列で行列

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

または，この行列の行，列を入れかえたものであるから補題3.15より位数3のアフィン平面はすべて同型である．

A を位数4とする．このときMは 12×4 行列で，2点を通る直線がただ1つ存在することより第1列と第2列を定め，さらに行列 M についての性質，定理 3.14 (1) より第1行を定めて

$$M=\begin{pmatrix} 1&2&3&4\\ 1&3&&\\ 1&4&&\\ 2&1&&\\ 2&3&&\\ 2&4&&\\ 3&1&*&\\ 3&2&&\\ 3&4&&\\ 4&1&&\\ 4&2&&\\ 4&3&& \end{pmatrix}$$

をうる．このとき行列Mについての性質（1），（2）を用いて＊の所は一意的に決まり

$$M=\begin{pmatrix} 1&2&3&4\\ 1&3&4&2\\ 1&4&2&3\\ 2&1&4&3\\ 2&3&1&4\\ 2&4&3&1\\ 3&1&2&4\\ 3&2&4&1\\ 3&4&1&2\\ 4&1&3&2\\ 4&2&1&3\\ 4&3&2&1 \end{pmatrix}$$

となる．したがって位数4のアフィン平面は補題3.15よりすべて同型である．□

系 3.17　位数2,3,4の射影平面がただ1つ存在する．

［証 明］　$PG(2,2)$，$PG(2,3)$，$PG(2,4)$ はそれぞれ位数 2,3,4 の射影平面である．Dを位数2,3または4の射影平面とする．Dの任意の直線に関する外部構造は位数2,3または4のアフィン平面であるから，定理 3.16 よりそれぞれ $AG(2,2)$，$AG(2,3)$ または $AG(2,4)$ である．したがって定理3.11より位数2,3または4の射影平面はそれぞれ $PG(2,2)$，$PG(2,3)$，$PG(2,4)$ に同型である．□

位数nの射影平面は存在してもただ1つであるとはいえない．たとえば位数9のとき，$PG(2,9)$ と同型でないものが存在する．

§4. W_{10}, W_{11}, W_{12} の一意性と自己同型群

補題 4.1　$D=(\Omega,\mathfrak{B})$, $D'=(\Omega',\mathfrak{B}')$ を結合構造, $p\in\Omega, p'\in\Omega'$ とする. $\Omega-\{p\}$ から $\Omega'-\{p'\}$ への全単射 φ でつぎの条件をみたすものが存在すれば, D と D' は同型である.

(1)　D の $\{p\}$ に関する内部構造を D_p, D' の $\{p'\}$ に関する内部構造を $D'_{p'}$ とすると, φ は D_p と $D'_{p'}$ の間の同型を与える.

(2)　$\mathfrak{B}_0=\{B\in\mathfrak{B}\,|\,p\notin B\}$, $\mathfrak{B}_0'=\{B'\in\mathfrak{B}'\,|\,p'\notin B'\}$ とすると $\mathfrak{B}_0{}^{\varphi}=\mathfrak{B}_0'$ である.

[証明]　写像 $\bar{\varphi}$; $\Omega\to\Omega'$ を $p^{\bar{\varphi}}=p', q^{\bar{\varphi}}=q^{\varphi}(q\in\Omega-\{p\})$ により定義する. このとき $\bar{\varphi}$ は明らかに Ω から Ω' への全単射である. いま D_p のブロックの集合を $\mathfrak{C}$, $D'_{p'}$ のブロックの集合を $\mathfrak{C}'$ とする. このとき p を通る D のブロックの集合は $\mathfrak{B}_{(p)}=\{\{p\}\cup C\,|\,C\in\mathfrak{C}\}$ であり, p' を通る D' のブロックの集合は $\mathfrak{B}'_{(p')}=\{\{p'\}\cup C'\,|\,C'\in\mathfrak{C}'\}$ である. φ は (1) より D_p から $D'_{p'}$ への同型写像であるから, $\mathfrak{C}^{\varphi}=\mathfrak{C}'$ であり $p^{\bar{\varphi}}=p'$ より $\mathfrak{B}^{\bar{\varphi}}_{(p)}=\mathfrak{B}'_{(p')}$ である.

また p を通らない D のブロックの集合は $\mathfrak{B}_0$ で p' を通らない D' のブロックの集合は $\mathfrak{B}_0'$ で (2) より $\mathfrak{B}_0{}^{\bar{\varphi}}=\mathfrak{B}_0{}^{\varphi}=\mathfrak{B}_0'$ である. したがって $\mathfrak{B}^{\bar{\varphi}}=\mathfrak{B}'$ となり $\bar{\varphi}$ は D と D' の同型を与える. □

Witt は 3-(10, 4, 1) デザイン, 4-(11, 5, 1) デザイン, 5-(12, 6, 1) デザインはそれぞれ W_{10}, W_{11}, W_{12} に限ることを示したが, このことを Lüneburg の方法にそって証明する.

補題 4.2　$D=(\Omega,\mathfrak{B})$ を位数3のアフィン平面, すなわち 2-(9, 3, 1) デザインとする. D において異なる2点 p_1, p_2 を通る直線を $\overline{p_1p_2}$, $\mathfrak{B}$ の異なる2直線 l_1, l_2 の交点を $l_1\cap l_2$ と書く. また同一直線上にある点を共線であるという. さらにいずれの3点も共線でない4点 p_1, p_2, p_3, p_4 を D の4角形 $p_1p_2p_3p_4$ といい, 4角形 $p_1p_2p_3p_4$ の2点ずつを通る2直線の組 $\overline{p_{i_1}p_{i_2}}$, $\overline{p_{i_3}p_{i_4}}$, $\{i_1, i_2, i_3, i_4\}=\{1, 2, 3, 4\}$ を4角形の対辺とよぶことにする.

このときつぎの (I) から (IV) が成り立つ.

(I)　$\mathfrak{B}$ は3個の直線からなる4個の平行線類　$L^{(i)}=\{l_1{}^{(i)},\ l_2{}^{(i)},\ l_3{}^{(i)}\}$

$(i=1,2,3,4)$ よりなる．

［証 明］ 補題3.5より $|\mathfrak{B}|=12$ である．さらに注 3.7 より各平行線類は3個の直線よりなる．したがって$\mathfrak{B}$は4個の平行線類よりなる． □

(II) 4角形の3組の対辺のうち，2組は平行2直線よりなり，1組が相交わる2直線よりなる．したがって4角形に対して相交わる2直線が一意的に決まり，4角形はこの2直線上の交点を除いた4点である．

逆に相交わる2直線上の交点を除いた4点は4角形である．

［証 明］ 4角形の2点を結んでできる直線は $\binom{4}{2}=6$ 個存在し，それらは3組の対辺を作る．ここで3組の対辺のうち2組が交わる2直線よりなるとすると，この2組の対辺を作る4個の直線と残りの1組の対辺を作る1つの直線の5個の直線は，いずれの2つも交わりしたがって異なる平行線類に属する．しかしこのことは平行線類が4個であることに反する．したがって3組の対辺がすべて平行な2直線よりなるか，3組のうち1組だけが交わる2直線よりなる．

いま3組の対辺がすべて平行2直線よりなるとすると，これら6個の直線は4角形の4点以外では交わらない．したがって各直線は3点を含むことより，Ω に少なくとも10点が存在し $|\Omega|=9$ に反する．以上より対辺のちょうど1組が交わる2直線よりなる．さらに1つの直線は3点を含むからこの交わる対辺の交点を除いた4点が4角形を作る．

逆に相交わる2直線上の交点を除いた4点は，いずれの3点も共線でないから，4角形を作る． □

(III) Dにおける4角形の集合を $\mathfrak{B}_0$ とし，相交わる2直線 l_1, l_2 により決まる4角形を (l_1, l_2) と書く．さらにつぎの4角形の集合 $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$ を4角形類とよぶ．

$$\mathfrak{C}_1=\{(l_i^{(1)}, l_j^{(2)})\,|\,i,j=1,2,3\}\cup\{(l_i^{(3)}, l_j^{(4)})\,|\,i,j=1,2,3\},$$
$$\mathfrak{C}_2=\{(l_i^{(1)}, l_j^{(3)})\,|\,i,j=1,2,3\}\cup\{(l_i^{(2)}, l_j^{(4)})\,|\,i,j=1,2,3\},$$
$$\mathfrak{C}_3=\{(l_i^{(1)}, l_j^{(4)})\,|\,i,j=1,2,3\}\cup\{(l_i^{(2)}, l_j^{(3)})\,|\,i,j=1,2,3\}.$$

このときつぎのことが成り立つ．

(i) $\mathfrak{B}_0=\mathfrak{C}_1\cup\mathfrak{C}_2\cup\mathfrak{C}_3$（互いに素）で，$|\mathfrak{C}_1|=|\mathfrak{C}_2|=|\mathfrak{C}_3|=18$ である．

(ii) Ω の共線でない異なる3点に対して，この3点を含む4角形がちょうど3個存在して，$\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ に1つずつ属す．

［証 明］ (i) (II) より $\mathfrak{B}_0=\mathfrak{C}_1\cup\mathfrak{C}_2\cup\mathfrak{C}_3$（互いに素）である．また $|\mathfrak{C}_i|=3\cdot3\cdot2$

$=18$ である.

(ii) 共線でない異なる3点 p_1, p_2, p_3 をとる. 3つの直線 $\overline{p_1p_2}$, $\overline{p_1p_3}$, $\overline{p_2p_3}$ は互いに交わる直線であるから異なる平行線類に属する. したがってこれら3直線のいずれをも含まない平行線類がちょうど1つ存在し, これを $L^{(i)}$ とする. $L^{(i)}$ の3直線はそれぞれ p_1, p_2, p_3 を通り, $p_1 \in l_1^{(i)}, p_2 \in l_2^{(i)}, p_3 \in l_3^{(i)}$ としてよい. このとき $(l_1^{(i)}, \overline{p_2p_3})$, $(l_2^{(i)}, \overline{p_1p_3})$, $(l_3^{(i)}, \overline{p_1p_2})$ は p_1, p_2, p_3 を含む異なる4角形で, $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$ に1つずつ属する.

ここで直線 $\overline{p_1p_2}$, $\overline{p_1p_3}$, $\overline{p_2p_3}$ のいずれの上にもない Ω の点は3個だから, p_1, p_2, p_3 を含む4角形は上の3個のみである. □

(IV) Dはアフィン平面 $AG(2,3)$ に同型であり, $G=\mathrm{Aut}\ D$ は位数 $9 \cdot 8 \cdot 6$ で4角形の集合$\mathfrak{B}_0$上可移に作用する. さらにGは4角形類の集合 $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ 上3次の対称群として作用する.

［証 明］ 定理 3.16 よりDはアフィン平面 $AG(2,3)$ としてよい. したがって定理 3.12 より $|G|=|P\Gamma L(2,3)|\cdot 3^2 \cdot (3-1)=9\cdot 8\cdot 6$ でΩ上2重可移である. これより任意の異なる2点 p, p' に対して $H=G_{p\,p'}$ とおくと $|H|=6$ である. 直線 $\overline{pp'}$ 上にない任意の点 p'' に対して $H_{p''}$ は直線 $\overline{pp'}$, $\overline{pp''}$, $\overline{p'p''}$ を固定し, したがってこれらの直線を含む平行線類を固定する. ここでこれら3直線は交わるから, 異なる平行線類に属し, Dは4個の平行線類をもつから, $H_{p''}$ は平行線類をすべて固定する. したがって定理 3.12 で示したように $H_{p''}$ は定理 3.12 の Frobenius 群Lに含まれ, さらに $H_{p''}$ は p, p', p'' を固定するから $H_{p''}=1$ である. したがって $|H|=6$ であるからHは直線 $\overline{pp'}$ 上の3点を除く6点の上で正則である.

$(\overline{p_1p_2}, \overline{p_3p_4})$, $(\overline{q_1q_2}, \overline{q_3q_4})$ を D の任意の4角形とする. G は Ω 上2重可移だから $x=\begin{pmatrix} p_1 & p_2 & \cdots \\ q_1 & q_2 & \cdots \end{pmatrix}$ なる元 $x \in G$ が存在する. このとき $\overline{p_1p_2} \cap \overline{p_3p_4}=p$, $\overline{q_1q_2} \cap \overline{q_3q_4}=q$ とすると $p^x=q$ である. いま $p_3{}^x=q_3'$, $p_4{}^x=q_4'$ とする. 上に示したように $G_{q_1q_2}$ は $\Omega-\{q_1, q_2, q\}$ 上可移だから $q_3'^y=q_3$ なる元 $y \in G_{q_1q_2}$ が存在する. このとき $\overline{qq_3'}^y=\overline{qq_3}$ となり, $q_4' \in qq_3'$, $q_4 \in qq_3$ より $q_4'^y=q_4$ である. したがってxyは4角形$(\overline{p_1p_2}, \overline{p_3p_4})$ を4角 $(\overline{q_1q_2}, \overline{q_3q_4})$ にうつし, これよりGは$\mathfrak{B}_0$上可移に作用する.

また定理 3.12 よりGは平行線類の集合 $\{L^{(1)}, L^{(2)}, L^{(3)}, L^{(4)}\}$ 上 $P\Gamma L(2,3)$ で補題 2;10.11 より対称群 S_4 に同型である. したがって4角形類の集合 $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ にGは作用する. $\{L^{(1)}, L^{(2)}, L^{(3)}, L^{(4)}\}$ 上 $(L^{(1)})(L^{(2)})(L^{(3)}\ L^{(4)})$ および $(L^{(2)})(L^{(3)})(L^{(1)}\ L^{(4)})$ であるGの元は $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ 上それぞれ $(\mathfrak{C}_1)(\mathfrak{C}_2\ \mathfrak{C}_3)$, $(\mathfrak{C}_1\ \mathfrak{C}_2)(\mathfrak{C}_3)$ である

から，Gは $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ 上対称群 S_3 である．□

補 題 4.3 $D=(\Omega, \mathfrak{B})$ を 3-(10, 4, 1) デザイン，$p\in\Omega$，$\mathfrak{C}$をpを含まない $\mathfrak{B}$ のブロックの集合とする．このとき D_p は位数3のアフィン平面で，D_p の4角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ とすると，$\mathfrak{C}$ は $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ のうちの1つに一致する．

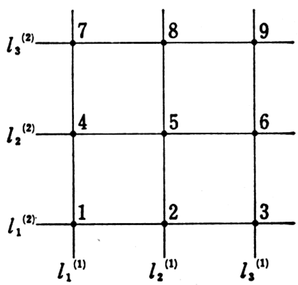
［証 明］ D_p は定理 2.1 より 2-(9, 3, 1) デザインで，したがって位数3のアフィン平面である．

Dにおいてpを含むブロックの集合は $\{\{p\}\cup l \mid l$ は D_p の直線$\}$ である．Dは会合数1の3-デザインであるから，pを通らないDのブロック，すなわち$\mathfrak{C}$のブロックはいずれの3点も D_p の直線を作らない4点よりなり，したがって D_p の4角形である．定理 2.8 より $|\mathfrak{B}|=\dfrac{10\cdot 9\cdot 8}{4\cdot 3\cdot 2}=30$ でpを通るブロックの個数は 12 である．したがって $|\mathfrak{C}|=30-12=18$ である．

D_p の平行線類を $L^{(i)}=\{l_1^{(i)}, l_2^{(i)}, l_3^{(i)}\}$ $(i=1,2,3,4)$ とし，$L^{(1)}$ の直線と $L^{(2)}$ の直線との交点に 3-3 図のように番号をうつ．このとき $\Omega=\{p, 1, 2, \cdots, 9\}$ で，$L^{(3)}$ と $L^{(4)}$ の直線を

$l_1^{(3)}=\{1, 5, 9\}$，　$l_2^{(3)}=\{2, 6, 7\}$，　$l_3^{(3)}=\{3, 4, 8\}$，
$l_1^{(4)}=\{1, 6, 8\}$，　$l_2^{(4)}=\{2, 4, 9\}$，　$l_3^{(4)}=\{3, 5, 7\}$

としてよい．



3-3 図

$\{1, 2, 4\}$ は D_p の直線ではないから，$\{1, 2, 4\}$ を含むDのブロックは$\mathfrak{C}$の元である．D_p において $\{1, 2, 4\}$ を含む4角形は補題 4.2 (III) より3個存在し，$\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$ に1つずつ属する．したがって $\{1, 2, 4\}$ を含むDのブロックを $\{1, 2, 4, 5\}=(l_1^{(3)}, l_2^{(4)})\in\mathfrak{C}_1$ としてよい．ここで $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$ を作る4角形は補題 4.2 (III) の通りとする．

4角形 $\{1, 2, 4, 5\}$ と2点のみを共有する$\mathfrak{C}$の元をしらべる．まず1, 2のみを共有する4角形は

$$(l_3^{(1)}, l_1^{(2)})=\{1, 2, 6, 9\},\qquad (l_2^{(3)}, l_1^{(4)})=\{1, 2, 7, 8\},$$
$$(l_1^{(1)}, l_2^{(4)})=\{1, 2, 7, 9\},\qquad (l_2^{(1)}, l_1^{(3)})=\{1, 2, 8, 9\}$$

である．一方Dにおいて与えられた2点を通るブロックの個数は定理 2.8 より $\dfrac{8}{2}=4$ 個である．したがって $\{1, 2\}$ を含むDのブロックは $\{p, 1, 2, 3\}$, $\{1, 2, 4, 5\}$ 以外に上の4角形のうちのちょうど2個で，それらの共有点は 1, 2 のみである．すなわち $(l_3^{(1)}, l_1^{(2)})$,

$(l_2^{(3)}, l_1^{(4)})$ がDのブロックになり共に D_p の $\mathfrak{C}_1$ に属する．

4 角形 $\{1,2,4,5\}$ の平行な対辺の 1 つの直線を作る 2 点 $\{4,5\}$, $\{1,4\}$ または $\{2,5\}$ を含む$\mathfrak{C}$ の元は $\{1,2,4,5\}$ 以外にそれぞれ 2 個ずつ存在するが，$\{1,2\}$ の場合と同様にしてそれらはすべて $\mathfrak{C}_1$ の異なる元である．

つぎに 4 角形 $\{1,2,4,5\}$ の相交わる対辺の 1 つの直線を作る 2 点 1,5 をとる．このとき 1,5 のみを共有する 4 角形は

$$(l_2^{(1)}, l_1^{(2)}) = \{1,5,3,8\},\qquad (l_1^{(1)}, l_2^{(2)}) = \{1,5,6,7\},$$
$$(l_3^{(1)}, l_1^{(3)}) = \{1,5,3,6\},\qquad (l_3^{(2)}, l_1^{(3)}) = \{1,5,7,8\}$$

で，このうちちょうど 2 個が$\mathfrak{C}$の元である．さらに先に求めた$\mathfrak{C}$の元 $\{1,2,7,8\}$ との共有点が 2 個以下でかつ互いに $\{1,5\}$ のみを共有するものは $(l_1^{(1)}, l_2^{(2)})$, $(l_2^{(1)}, l_1^{(2)})$ の 2 個である．すなわちこの 2 個の 4 角形が$\mathfrak{C}$の元となり，$\mathfrak{C}_1$に属する．同様にして 2 点 2,4 を含む$\mathfrak{C}$の元が $\{1,2,4,5\}$ 以外に 2 つ決まり $\mathfrak{C}_1$ に属する．以上より異なる $\mathfrak{C}$ の元が $1+6\times 2=13$ 個決まり，それらはすべて $\mathfrak{C}_1$に属する．

いま$\mathfrak{C}_1$と異なる $\mathfrak{C}_i$ の元Cが$\mathfrak{C}$に属すると，同様にしてCより13個の $\mathfrak{C}_i$ の元が$\mathfrak{C}$に属する．ここで $\mathfrak{C}_1 \cap \mathfrak{C}_i = \phi$ であるから，$13+13 \leqq |\mathfrak{C}|$ となり $|\mathfrak{C}|=18$ に反する．

以上より $\mathfrak{C} \subseteqq \mathfrak{C}_1$ となり $|\mathfrak{C}| = |\mathfrak{C}_1| = 18$ であるから $\mathfrak{C} = \mathfrak{C}_1$ である．□

定 理 4.4　3-(10,4,1) デザインは W_{10} に同型である．

［証 明］ 定理 2.9 より W_{10} は 3-(10,4,1) デザインである．いま $D=(\Omega,\mathfrak{B})$, $D'=(\Omega',\mathfrak{B}')$ を任意の 3-(10,4,1) デザインとし $p\in\Omega, p'\in\Omega'$ とする．

$D_p, D'_{p'}$ は共に 2-(9,3,1) デザインで定理 3.16 より同型である．いま写像φをD_pから $D'_{p'}$ への同型とする．$\mathfrak{B}_0=\{B\in\mathfrak{B}\,|\,p\notin B\}, \mathfrak{B}_0'=\{B'\in\mathfrak{B}'\,|\,p'\notin B'\}$ とおくと $B\in\mathfrak{B}_0$ は $\Omega-\{p\}$ の部分集合として B^φ が定義でき，$B^\varphi \subseteqq \Omega'-\{p'\}$ である．$\mathfrak{B}_0^\varphi = \{B^\varphi\,|\,B\in\mathfrak{B}_0\} = \mathfrak{B}_0''$ とおく．補題 4.3 より $\mathfrak{B}_0$, $\mathfrak{B}_0'$ はそれぞれ D_p, $D'_{p'}$ の 1 つの 4 角形類であり，φは D_p から $D'_{p'}$ への同型であるから $\mathfrak{B}_0''$ も 1 つの 4 角形類である．さらに補題 4.2 (IV) より $\mathfrak{B}_0''^{\psi}=\mathfrak{B}_0'$ である $\psi\in \mathrm{Aut}\,D'_{p'}$ が存在する．したがって $\varphi\psi$ は $\Omega-\{p\}$ から $\Omega'-\{p'\}$ への全単射で，$\mathfrak{B}_0^{\varphi\psi}=\mathfrak{B}_0'$ であるから補題 4.1 よりDと D' は同型である．□

Dを位数 3 のアフィン平面，Dの 4 角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ とする．いまDの 4 角形 (l,l') に対して $l\cup l' = (l,l')\cup\{l\cap l'\}$ は 5 点からなり，$\overline{\mathfrak{C}_i} = \{l\cup l'\,|\,(l,l')\in\mathfrak{C}_i\}$ $(i=1,2,3)$ を 5 角形類とよぶことにする．

定 理 4.5　4-(11,5,1) デザインは W_{11} に同型である．

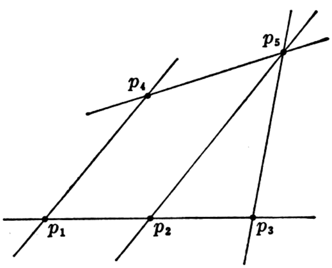
［証 明］ 定理2.6より W_{11} は 4-(11,5,1) デザインである.

$D=(\Omega,\mathfrak{B})$ を 4-(11,5,1) デザイン，$p,q(\neq)\in\Omega$ とすると D_p, D_q は 3-(10,4,1) デザイン，$D_{p,q}$ は位数3のアフィン平面である.

定理2.8より $|\mathfrak{B}|=\dfrac{11\cdot10\cdot9\cdot8}{5\cdot4\cdot3\cdot2}=66$ であり，pを含むブロックは $\dfrac{10\cdot9\cdot8}{4\cdot3\cdot2}=30$ 個で各ブロックは $\{p\}$ と D_p のブロックの和集合である．さらに D_p のブロックは補題 4.3 より $\{q\}$ と $D_{p,q}$ の直線の和集合である 12 個と，$D_{p,q}$ の1つの4角形類（$\mathfrak{C}_1$ とする）の4角形である18個よりなる．またpを含まないDのブロックのうちqを含むブロックは $\{q\}$ と $D_{p,q}$ の $\mathfrak{C}_1$ と異なる4角形類（$\mathfrak{C}_2$ とする）の4角形の和集合で18個存在する.

以上よりpもqも含まないDのブロックは $66-30-18=18$ 個で，$D_{p,q}$ の5点よりなる．いまこのブロックを5角形とよび5角形の集合を $\overline{\mathfrak{C}}$ とおく．ここで5角形が $D_{p,q}$ の4角形を部分集合として含むならば，Dは会合数1の4-デザインであるから，この4角形は $\mathfrak{C}_1, \mathfrak{C}_2$ と異なる4角形類 $\mathfrak{C}_3$ に属する.

いまアフィン平面 $D_{p,q}$ で考える．1つの4角形に対して4角形に含まれない $D_{p,q}$ の点は必ず4角形の2点を通る直線上にある．したがって $\{p_1,p_2,\cdots,p_5\}$ を5角形とすると同一直線上にある3点が存在し，これを p_1, p_2, p_3 とする．$\overline{p_4p_5}\,/\!\!/\,\overline{p_1p_2}$ とすると，$\{p_1,p_2,p_4,p_5\}$ および $\{p_1,p_3,p_4,p_5\}$ は共に4角形になり，この2つの4角形は3点 p_1, p_4, p_5 を共有する．したがって補題 4.2 (III) より，この2つの4角形は異なる4角形類に属し，5角形 $\{p_1,p_2,\cdots,p_5\}$ が4角形を含むならば $\mathfrak{C}_3$ の4角形に限ることに反する．したがって $\overline{p_4p_5}$ は $\overline{p_1p_2}$ と交わり交点を p_1 としてよい．すると $\{p_2,p_3,p_4,p_5\}$ は $\mathfrak{C}_3$ の4角形になり，5角形 $\{p_1,p_2,\cdots,p_5\}\in\overline{\mathfrak{C}}_3$ になる．



3-4 図

以上より $\overline{\mathfrak{C}}\subseteq\overline{\mathfrak{C}}_3$ となり，$|\overline{\mathfrak{C}}|=|\overline{\mathfrak{C}}_3|=18$ より $\overline{\mathfrak{C}}=\overline{\mathfrak{C}}_3$ となる．すなわち 4-(11,5,1) デザインDにおいて，$D_{p,q}$ に含まれるDの5角形全体の集合$\overline{\mathfrak{C}}$は，$D_{p,q}$ の4角形類 $\mathfrak{C}_3$ から定まる5角形類 $\overline{\mathfrak{C}}_3$ に一致する.

$D=(\Omega,\mathfrak{B})$ $D'=(\Omega',\mathfrak{B}')$ を任意の 4-(11,5,1) デザインとし，$p\in\Omega, p'\in\Omega'$ とする．D_p, $D'_{p'}$ は共に 3-(10,4,1) デザインで定理4.4より同型で，写像φを D_p から $D'_{p'}$ への同型とする．また $q\in\Omega-\{p\}$ とし，$q'=q^\varphi$ とする．$\mathfrak{B}_0=\{B\in\mathfrak{B}\mid p\notin B\}$，$\mathfrak{B}_0'=\{B'\in\mathfrak{B}'\mid p'\notin B'\}$ とおき，$D_{p,q}$ の4角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$, $D'_{p',q'}$ の4角形類を

$\mathfrak{C}_1'$, $\mathfrak{C}_2'$, $\mathfrak{C}_3'$ とする．このとき上に述べたことより，$\{p\}$ を含み $\{q\}$ を含まない D のブロックは $\{p\}$ と $\mathfrak{C}_1$ の4角形の和集合，$\{p'\}$ を含み $\{q'\}$ を含まない D' のブロックは $\{p'\}$ と $\mathfrak{C}_1'$ の4角形の和集合とし，

$$\mathfrak{B}_0 = \{\{q\} \cup C \mid C \in \mathfrak{C}_2\} \cup \overline{\mathfrak{C}}_3,$$

$$\mathfrak{B}_0' = \{\{q'\} \cup C' \mid C' \in \mathfrak{C}_2'\} \cup \overline{\mathfrak{C}}_3'$$

としてよい．これより $\mathfrak{C}_1^{\varphi} = \mathfrak{C}_1', \mathfrak{C}_2^{\varphi} = \mathfrak{C}'_{2'}, \mathfrak{C}_3^{\varphi} = \mathfrak{C}'_{3'}, \{2', 3'\} = \{2, 3\}$

$$\mathfrak{B}_0^{\varphi} = \{\{q'\} \cup C' \mid C' \in \mathfrak{C}'_{2'}\} \cup \overline{\mathfrak{C}'}_{3'}$$

となる．補題 4.2 (IV) より $\bar{\psi} \in \mathrm{Aut}\, D'_{p',q'}$ で $\mathfrak{C}'_1{}^{\bar{\psi}} = \mathfrak{C}_1'$, $\mathfrak{C}'_{2'}{}^{\bar{\psi}} = \mathfrak{C}_2'$, $\mathfrak{C}'_{3'\bar{\psi}} = \mathfrak{C}_3'$ となるものが存在する．いま ψ を q' を固定し $D'_{p',q'}$ 上 $\bar{\psi}$ と一致する $\Omega' - \{p'\}$ 上の置換とすると補題4,1 より $\psi \in \mathrm{Aut}\, D'_{p'}$ である．したがって $\varphi\psi$ は D_p から $D'_{p'}$ への同型で $\mathfrak{B}_0^{\varphi\psi} = \mathfrak{B}_0'$ となり，補題 4.1 より D と D' は同型である．∎

定理 4.6 5-(12, 6, 1) デザインは W_{12} に同型である．

［証明］ 定理2.6 より W_{12} は 5-(12, 6, 1) デザインである．

$D = (\Omega, \mathfrak{B})$ を 5-(12, 6, 1) デザイン，$p, q, r(\neq) \in \Omega$ とする．$D_{p,q,r}$ は位数3のアフィン平面で4角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$，5角形類を $\overline{\mathfrak{C}_1}, \overline{\mathfrak{C}_2}, \overline{\mathfrak{C}_3}$ とする．補題 2.8 より $|\mathfrak{B}| = \dfrac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = 132$ で，このうち p を含むブロックは $\dfrac{11 \cdot 10 \cdot 9 \cdot 8}{5 \cdot 4 \cdot 3 \cdot 2} = 66$ 個で $\{p\}$ と D_p のブロックの和集合である．したがって p を含むブロックを

$$\{\{p, q, r\} \cup l \mid l \text{ は } D_{p,q,r} \text{ の直線}\} \cup \{\{p, q\} \cup C \mid C \in \mathfrak{C}_1\} \cup \{\{p, r\} \cup C \mid C \in \mathfrak{C}_2\}$$
$$\cup \{\{p\} \cup \bar{C} \mid \bar{C} \in \overline{\mathfrak{C}_3}\}$$

としてよい．つぎに p を含まないブロックは $132 - 66 = 66$ 個で，p を含む上で定めたブロックより

$$\{\{q, r\} \cup C \mid C \in \mathfrak{C}_3\} \cup \{\{q\} \cup \bar{C} \mid \bar{C} \in \overline{\mathfrak{C}_2}\} \cup \{\{r\} \cup \bar{C} \mid \bar{C} \in \overline{\mathfrak{C}_1}\}$$
$$\cup \{\Omega - \{p, q, r\} \text{ の6点からなる } \mathfrak{B} \text{ の元}\}$$

となる．ここで D のブロックを作る $\Omega - \{p, q, r\}$ の6点を6角形，その集合を6角形類とよぶと6角形類は $66 - 18 \times 3 = 12$ 個の6角形よりなり，p を含まないブロックは，6角形を除きすべて p を含むブロックにより一意的に定まる．

いま位数3のアフィン平面 $D_{p,q,r}$ について考え，$\{p_1, p_2, \cdots, p_6\}$ を6角形とすると，この6点のうち共線である3点が必ず存在する．これを p_1, p_2, p_3 とする．直線 $\overline{p_4p_5}$ が直線 $\overline{p_1p_2}$ と交わるとその交点は p_1, p_2, p_3 のいずれかで $\{p_1, p_2, \cdots, p_5\}$ は5角形になり，この5点と $\{p, q, r\}$ の1点を含む D のブロックが存在するから，D が会合数1の5-デザインであることに反する．したがって $\overline{p_1p_2} /\!/ \overline{p_4p_5}$ であり，同様にして $\overline{p_1p_2} /\!/ \overline{p_4p_6}$

となり，p_4, p_5, p_6 は $\overline{p_1p_2}$ に平行な1つの直線を作る．位数3のアフィン平面は4個の平行線類をもち，各平行線類は3個の平行線よりなるから，平行2直線の組は全部で $\binom{3}{2}\cdot 4=12$ 個存在する．ここで6角形の個数も12であるから，任意の平行2直線上の6点が6角形となり，したがって p, q, r を含まないDのブロックは $D_{p,q,r}$ において一意的に決まる．

$D=(\Omega, \mathfrak{B}), D'=(\Omega', \mathfrak{B}')$ を任意の 5-(12, 6, 1) デザインとし，$p\in\Omega$, $p'\in\Omega'$ とする．$D_p, D'_{p'}$ は共に 4-(11, 5, 1) デザインで定理 4.5 より同型であり，写像φを D_p から $D'_{p'}$ への同型とする．pを含まないDのブロックはpを含むブロック，したがって D_p のブロック，により一意的に決まり，同様にp'を含まない D' のブロックは $D'_{p'}$ のブロックにより一意的に決まる．したがってpを含まないDのブロックはφによりp'を含まない D' のブロックに移り，補題4.1よりDと D' は同型である．□

定理 4.7 Aut $W_{12}=M_{12}$, Aut $W_{11}=M_{11}$ である．さらに Aut W_{10} $=P\Gamma L(2,9)$ で12次の Mathieu 群 M_{12} の2点の集合としての安定化群である．

［証明］ (i) $D=W_{10}, G=$ Aut W_{10} とおく．D は W_{12} の2点に関する内部構造であり，系1.5によって12次の Mathieu 群 M_{12} の2点の集合としての安定化群は $P\Gamma L(2,9)$ で $M_{12}\leqq$ Aut W_{12} より $G\geqq P\Gamma L(2,9)$ である．したがって $|G|\geqq |P\Gamma L(2,9)|=10\cdot9\cdot8\cdot2$ でGはDの点集合上3重可移である．

Dの点pに対して D_p は位数3のアフィン平面であるから，補題 4.2 (IV) により $|\mathrm{Aut}\ D_p|=9\cdot8\cdot6$ である．D_p の4角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ とし，補題4.3よりpを含まないDのブロックの集合を $\mathfrak{C}_1$ としてよい．Aut D_p は $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ に作用し，補題 4.2(IV) よりこの上で対称群 S_3 である．したがって Aut D_p における $\mathfrak{C}_1$ の安定化群 $(\mathrm{Aut}\ D_p)_{\mathfrak{C}_1}$ は $|(\mathrm{Aut}\ D_p)_{\mathfrak{C}_1}|=|\mathrm{Aut}\ D_p|/3=9\cdot8\cdot2$ である．一方Gにおける点pの安定化群 G_p は D_p 上 Aut D_p の部分群であり，さらにDの p を含まないブロック $\mathfrak{C}_1$ を固定するから，G_p は D_p 上 $(\mathrm{Aut}\ D_p)_{\mathfrak{C}_1}$ の部分群である．したがって $|G_p|\leqq|(\mathrm{Aut}\ D_p)_{\mathfrak{C}_1}|=9\cdot8\cdot2$ となり，$|G|=10\cdot|G_p|\leqq10\cdot9\cdot8\cdot2$ である．すなわち $|G|=10\cdot9\cdot8\cdot2$ となり $G=P\Gamma L(2,9)$ である．

(ii) $D=W_{11}$, $G=$Aut D とおくと $M_{11}\leqq G$ であり，$|G|\geqq11\cdot10\cdot9\cdot8$である．$p, q$ をDの異なる2点とすると，$D_{p,q}$は位数3のアフィン平面であるから，$|\mathrm{Aut}\ D_{p,q}|=9\cdot8\cdot6$ で G_{pq} は $D_{p,q}$ 上 Aut $D_{p,q}$ の部分群である．いま $D_{p,q}$ の4角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ とすると Aut $D_{p,q}$ は $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ 上対称群 S_3 であり，定理 4.5 の証明でみたように，G_{pq} は $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ を固定する．したがって $|G_{pq}|\leqq|\mathrm{Aut}\ D_{p,q}|/6=9\cdot8$

である．ここでGはDの点集合上4重可移であるから，$|G|=11\cdot10\cdot|G_{pq}|\leqq 11\cdot10\cdot9\cdot8$ となり $|G|=11\cdot10\cdot9\cdot8$ すなわち $G=M_{11}$ である．

(iii) $D=W_{12}, G=\mathrm{Aut}\ D$ とおくと $M_{12}\leqq G$ である．pをDの点とすると (ii) より D_p 上 $G_p\leqq \mathrm{Aut}\ D_p=M_{11}$ である．ここで M_{12} は M_{11} の可移拡大であるから $G=M_{12}$ である．□

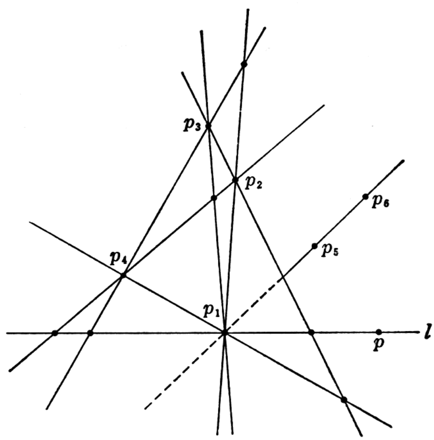
§ 5. W_{22}, W_{23}, W_{24} の一意性と自己同型群

Witt は前節と同じように，3-(22, 6, 1) デザイン，4-(23, 7, 1) デザイン，5-(24, 8, 1) デザインはそれぞれ W_{22}, W_{23}, W_{24} に限ることを示したが，このことを Lüneburg の方法にそって証明する．

補題 5.1 $D=(\Omega,\mathfrak{B})$ を位数4の射影平面すなわち 2-(21, 5, 1) デザインとする．Dにおいていずれの3点も共線でない4点および6点をそれぞれ4角形，6角形とよぶことにする．このときつぎの（I）から（X）の性質が成り立つ．

（I） 共線でない3点を含む6角形が3個，4角形を含む6角形が1個存在する．

［証明］ p_1, p_2, p_3 を共線でない3点とする．このとき3個の直線 $\overline{p_1p_2}$, $\overline{p_1p_3}$, $\overline{p_2p_3}$ 上に12点が存在し，残りの9点から任意の1点 p_4 をとる．$\{p_1, p_2, p_3, p_4\}$ は4角形である．このとき6個の直線 $\overline{p_ip_j}$ $(i, j=1, 2, 3, 4)$ 上に19点が存在し，残りの2点を p_5, p_6 とする．いま直線 $\overline{p_5p_6}$ 上に点 p_i $(i\neq 5, 6)$ たとえば p_1 が存在するとする．p_1 を通る直線は5個存在するから，4個の直線 $\overline{p_1p_i}$ $(i=2, 3, 4, 5)$ 以外に1個存在しこれを l とする．l は5点を含むから l と $\overline{p_2p_3}$, $\overline{p_2p_4}$, $\overline{p_3p_4}$ との交点および p_1 と異なる点が l 上に存在しこれを p とする．このとき p は直線 $\overline{p_i\,p_j}$ $(i, j=1, 2, 3, 4)$ のいずれの上にもなく，かつ p_5, p_6 と異なる点となり矛盾である．したがって p_1, p_5, p_6 は共線でなく $\{p_1, p_2, \cdots, p_6\}$ は6角形である．



3-5 図

さらに4角形 $\{p_1, p_2, p_3, p_4\}$ に対して一意的に2点 p_5, p_6 が定まるから，4角形 $\{p_1, p_2, p_3, p_4\}$ を含む6角形は $\{p_1, p_2, \cdots, p_6\}$ のみである．つぎに3点 p_1, p_2, p_3 に対して直線 $\overline{p_1p_2}$, $\overline{p_1p_3}$, $\overline{p_2p_3}$ のいずれの上にもない9点が存在するから，その任意の1点に対してこの点と p_1, p_2, p_3 を含む6角形が一意的に決まり，したがって p_1, p_2, p_3 を含む6角形がちょうど3個存在する．□

(II) Dの6角形の集合を $\mathfrak{B}_0$ とすると $|\mathfrak{B}_0| = 168$ である．

［証 明］ 4角形はその作り方より考えて全部で

$$\frac{21 \cdot 20 \cdot (21-5)(21-12)}{4 \cdot 3 \cdot 2 \cdot 1} = 21 \cdot 20 \cdot 6 \quad \text{個}$$

である．また6角形は $\binom{6}{4} = 15$ 個の4角形を含み，(I) よりこの15個の4角形はただ1つの同じ6角形に含まれる．したがって $|\mathfrak{B}_0| = \dfrac{21 \cdot 20 \cdot 6}{15} = 168$ である．□

(III) $D = PG(2,4)$, $\mathrm{Aut}\, D = P\Gamma L(3,4)$ である．

［証 明］ 系 3.17 より $D = PG(2,4)$ である．したがって定理3.9より $\mathrm{Aut}\, D = P\Gamma L(3,4)$ である．□

(IV) $\bar{G}$ を $\bar{\Omega} = \{1, 2, \cdots, 24\}$ 上の Mathieu 群 M_{24} とすると，$\bar{G}_{(1,2,3)}$ は $\{4, 5, \cdots, 24\}$ 上 $P\Gamma L(3,4)$ である．

［証 明］ $\Omega = \{4, 5, \cdots, 24\}$ を $PG(2,4)$ とみなすとき，定理 1.6 より $(\bar{G}_{1\,2\,3})^{\Omega} = PSL(3,4)$ である．また定理1.6における

a_4: 1を固定し $2 \leftrightarrow 3$, $[\lambda_1, \lambda_2, \lambda_3] \mapsto [\lambda_1^2, \lambda_2^2, \rho\lambda_3^2]$

a_5: 3を固定し $1 \leftrightarrow 2$, $[\lambda_1, \lambda_2, \lambda_3] \mapsto [\lambda_1^2, \lambda_2^2, \lambda_3^2]$

をとると $\bar{G}_{(1,2,3)} = \langle \bar{G}_{1\,2\,3}, a_4, a_5 \rangle$ である．Aut $GF(4)$ の元 $\theta : \rho \mapsto \rho^2$ $(\rho \in GF(4))$ に対して $P\Gamma L(3,4)$ の元 $[\theta] : [\lambda_1, \lambda_2, \lambda_3] \mapsto [\lambda_1^2, \lambda_2^2, \lambda_3^2]$ をとると，$PG(2,4)$ 上

$$[\lambda_1, \lambda_2, \lambda_3]^{a_4} = [\lambda_1, \lambda_2, \lambda_3]^{[\theta]\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \rho \end{bmatrix}}$$

$$[\lambda_1, \lambda_2, \lambda_3]^{a_5} = [\lambda_1, \lambda_2, \lambda_3]^{[\theta]}$$

となり，$a_4^{\Omega}, a_5^{\Omega} \in P\Gamma L(3,4)$ である．よって (III) より $(\bar{G}_{(1,2,3)})^{\Omega} \leqq \mathrm{Aut}\ PG(2,4)$ である．一方 $|\bar{G}_{(1,2,3)} : \bar{G}_{1\,2\,3}| = 6$, $|P\Gamma L(3,4) : PSL(3,4)| = 6$ であるから，$(\bar{G}_{(1,2,3)})^{\Omega} = P\Gamma L(3,4)$ となる．□

以下では射影平面 $D = (\Omega, \mathfrak{B})$ は $\Omega = \{4, 5, \cdots, 24\}$ とし，系 1.8 で定義された生成元をもつ $\bar{G}_{(1,2,3)}$ をΩに制限した $(G_{(1,2,3)})^{\Omega}$ を (III), (IV) より $\mathrm{Aut}D$とし，$G = (\bar{G}_{(1,2,3)})^{\Omega}, K = (\bar{G}_{1\,2\,3})^{\Omega}$ とおく．ここで $x \in \bar{G}_{(1,2,3)}$ に対して

x^{Ω}を単にxと書き，$i,j(\neq)\in\Omega$ に対してi,jを通る$\mathfrak{B}$の直線を $\overline{i,j}$ と書く．

(V) (i) xを $|F(x)|=5$ であるKの位数2の元とすると，$F(x)$ は $\mathfrak{B}$ の直線である．

(ii) y を $F(y)=\{i,j,k\}$ であるKの位数3の元とすると，yの巡回表示は6個の3-巡回置換をもち，i,j,k は共線ではない．また $\overline{i,j}-\{i,j\}$ の3点，$\overline{i,k}-\{i,k\}$ の3点，$\overline{j,k}-\{j,k\}$ の3点および $\{i,j,k\}$ を含む3つの6角形における i,j,k を除いた残りの3点は，それぞれがyの3-巡回置換を作る．

［証 明］ (i) xを $F(x)=\{i_1,i_2,\cdots,i_5\}$ であるKの位数2の元とする．直線 $\overline{i_1,i_2}$ をxは固定し，$\overline{i_1,i_2}$ は5点よりなるから $i_3\in\overline{i_1,i_2}$ としてよい．もし $i_4\notin\overline{i_1,i_2}$ であれば，異なる2つの直線 $\overline{i_1,i_4}$，$\overline{i_2,i_4}$ は同様にして $F(x)$ の残りの1点 i_5 を共に含み，$\overline{i_1,i_4}\neq\overline{i_2,i_4}$ に反する．したがって $i_4\in\overline{i_1,i_2}$ となり，同様にして $i_5\in\overline{i_1,i_2}$ となり $F(x)$ は$\mathfrak{B}$の直線である．

(ii) 補題1.7よりKは3点を固定する位数3の元をもつ．いまyを $F(y)=\{i,j,k\}$ であるKの位数3の元とすると，yは $|\Omega-\{i,\ j,\ k\}|/3=6$ 個の3-巡回置換をもつ．直線 $\overline{i,j}$ をyは固定し，$\overline{i,j}$ は5点よりなるから $\overline{i,j}$ はyの1つの 3-巡回置換を作る3点を含む．したがって $\overline{i,j}$，$\overline{i,k}$，$\overline{j,k}$ は異なる3直線で，それぞれ異なるyの3-巡回置換を作る3点を含む．

いま $(j_1\ j_2\ j_3)$ を j_1,j_2,j_3 が直線 $\overline{i,j}$，$\overline{i,k}$，$\overline{j,k}$ のいずれにも含まれないyの残りの3つの3-巡回置換の任意の1つとする．j_1，j_2，j_3 が共線であれば $\overline{j_1,j_2}$ をyは固定し，$\overline{j_1,j_2}$ は5点よりなるから $\overline{j_1,j_2}$ は $F(y)$ の2点を含み，j_1，j_2 のとり方に反する．したがって j_1,j_2,j_3 は共線でない．さらにもし i,j_1,j_2 が共線であれば $\overline{i,j_2}^{\,y}\supset\{i,j_1,j_2\}^y=\{i,j_2,j_3\}$ より $\overline{i,j_2}^{\,y}=\overline{i,j_2}\supset\{j_1,j_2,j_3\}$ となり矛盾である．同様にして i,j_1,j_3 および i,j_2,j_3 は共線でなく，したがって i,j_1,j_2,j_3 は4角形を作る．(I)より4角形 $\{i,j_1,j_2,\ j_3\}$ を含む6角形はただ1つだからyはこの6角形を固定し，したがってこの6角形は $\{i,j,k,j_1,j_2,j_3\}$ である．さらに(I)より $\{i,j,k\}$ を含む6角形は3つ存在し，i,j,k 以外の3点がそれぞれyの異なる3-巡回置換を作る．□

(VI) **Kは$\mathfrak{B}_0$上3つの軌道 $\mathfrak{C}_1$，$\mathfrak{C}_2$，$\mathfrak{C}_3$ をもち，$|\mathfrak{C}_1|=|\mathfrak{C}_2|=|\mathfrak{C}_3|=56$ である．また共線でない3点を含む3個の6角形は，$\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3$ に1つずつ属する．以下 $\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3$ を6角形類とよぶことにする．**

［証 明］ 系1.8のKの生成元cを用い(V)より4,5,9は共線でない．いまi,j,kを共

線でない任意の3点とする．定理1.6よりKはΩ上2重可移だから，$\{i,j,k\}^x=\{4,5,k'\}$である元 $x\in K$ が存在する．このとき $k'\notin\overline{4,5}$ で $\overline{4,5}=F(b_1)$ より $k'\in\{9,10,\cdots,24\}$である．補題1.7より $K_{F(b_1)}$ は $\{9,10,\cdots,24\}$ 上可移であるから $\{4,5,k'\}^y=\{4,5,9\}$である $y\in K_{F(b_1)}$ が存在する．すなわち $\{i,j,k\}^{xy}=\{4,5,9\}$ となりKは共線でない3点上可移であり，(V) より $c^{(xy)^{-1}}$ は i,j,k を含む6角形の上で3-巡回置換をもつ．

いま $\Delta=\{i_1,i_2,\cdots,i_6\}$ を6角形とすると，Δの任意の3点 $i_{1'},i_{2'},i_{3'}$ に対してcと共役でΔ上 $(i_{1'})(i_{2'})(i_{3'})(i_{4'}\ i_{5'}\ i_{6'})$ である元が存在する．したがって補題 2; 3.10 (1)より K^Δ は交代群 A_6 を含む．いまΔ上4点を固定し互換1つよりなる元が存在すれば，4点以上を固定する Kの元 $(\neq 1)$ は位数2で (V) よりΔの4点は共線になりΔが6角形であることに反する．したがって $K^\Delta=A_6$ である．また $|\Delta|=6$ であるから$K_\Delta=1$となり $|K_{(\Delta)}|=|K^\Delta|\cdot|K_\Delta|=|A_6|$ となる．系 2;4.4 よりΔを含む$\mathfrak{B}_0$上のK-軌道の長さは $|K|/|K_{(\Delta)}|=(21\cdot20\cdot3\cdot16)/(6\cdot5\cdot4\cdot3)=56$ となり，$\mathfrak{B}_0$は長さ56の3個の K-軌道よりなる．これを $\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3$ とおく．

Kは共線でない3点の集合の上で可移であり，共線でない3点を含む6角形はちょうど3個存在するから，1つずつ $\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3$ に属する．□

(VII) Gは $\{\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3\}$ に作用し，この上で対称群S_3である．

[証 明] KはGの正規部分群であるから，注 2; 5.2 より $\mathfrak{B}_0$ 上のK-軌道の集合$\{\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3\}$ にGは作用する．

(V) より $F(b_1)=\{4,5,6,7,8\}=\overline{4,5}$ である．これより $\overline{4,9}=\overline{4,5}^{a_1}=\{4,9,10,11,12\}$， $\overline{5,9}=\overline{4,9}^{a_2}=\{5,9,14,20,23\}$ である．ここで $F(c)=\{4,5,9\}$ であるから，(V) より

$$C_1=\{4,5,9,13,18,22\},\quad C_2=\{4,5,9,15,19,21\},\quad C_3=\{4,5,9,16,17,24\}$$

は $\{4,5,9\}$ を含む6角形で (VI) より $C_i\in\mathfrak{C}_i\ (i=1,2,3)$ としてよい．このとき$C_1{}^{a_4}=C_3,\ C_2{}^{a_4}=C_2,\ C_3{}^{a_4}=C_1$ であるから，a_4 は $\{\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3\}$ 上 $(\mathfrak{C}_1\ \mathfrak{C}_3)(\mathfrak{C}_2)$ である．さらに $C_1{}^{a_5}=C_1,\ C_2{}^{a_5}=C_3,\ C_3{}^{a_5}=C_2$ であるから，a_5 は $\{\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3\}$ 上$(\mathfrak{C}_1)(\mathfrak{C}_2\ \mathfrak{C}_3)$ である．したがってGは $\{\mathfrak{C}_1,\mathfrak{C}_2,\mathfrak{C}_3\}$ 上対称群はS_3として作用する．□

(VIII) $C\in\mathfrak{C}_i,\ C'\in\mathfrak{C}_j,\ |C\cap C'|\geqq 2$ とする．

(i) $i\neq j$ のとき $|C\cap C'|=3$ である．

(ii) $i=j, C\neq C'$のとき $|C\cap C'|=2$ でCと $C\cap C'$ のみを共有する6角形がちょうど3個存在し，すべて$\mathfrak{C}_i$に属する．

［証 明］ C と C' は少なくとも 2 点を共有する異なる 6 角形であるから，（I）より $|C\cap C'|=2$ または 3 である．

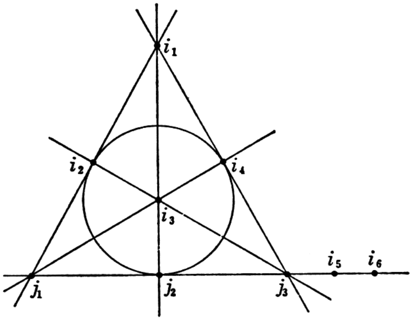
$|C\cap C'|=3$ であれば（VI）より $i\neq j$ である．したがって $|C\cap C'|=2$ とし，$C\cap C'=\{i_1,i_2\}$ とする．i_1,i_2 を含む 6 角形は $\dfrac{(21-5)(21-12)}{2}\Big/\dbinom{4}{2}=12$ 個でこのうち C と i_1,i_2 を含む 3 点を共有する 6 角形は $4\times2=8$ 個である．したがって C と i_1,i_2 のみを共有する 6 角形は $12-8-1=3$ 個である．$K_{i_1i_2}=\bar{K}$ とおき，C を含む $\bar{K}$-軌道 $C^{\bar{K}}$ に属する 6 角形は（VI）より共有点は i_1,i_2 のみである．ここで $\bar{K}$ は $\Omega-\overline{i_1,i_2}$ 上補題 1.7（2）より可移で，$|\Omega-\overline{i_1,i_2}|=16$ であるから $|C^{\bar{K}}|=16/4=4$ である．すなわち 2 点 i_1,i_2 のみを C と共有する 6 角形は $C^{\bar{K}}$ に属し，したがって C と同じ K-軌道 $\mathfrak{C}_i$ に属する．□

一般に $D=(\Omega,\mathfrak{B})$ を射影平面とし，$\Omega'\subset\Omega,\mathfrak{B}'=\{l\cap\Omega'\,|\,l\in\mathfrak{B},\ |l\cap\Omega'|\gneqq1\}$ による結合構造 $D'=(\Omega',\mathfrak{B}')$ がまた射影平面のとき D' を D の **部分平面** という．

以下位数 2 の D の部分平面（すなわち 2-(7,3,1)デザイン）を 7 角形ということにする．

（IX） $\{i_1,i_2,i_3,i_4\}$ を 4 角形とし，これを含む 6 角形を $\{i_1,i_2,\cdots,i_6\}$ とする．このとき $\{i_1,i_2,i_3,i_4\}$ を含む 7 角形 $\{i_1,i_2,i_3,i_4,j_1,j_2,j_3\}$ がただ 1 つ存在し，i_5,i_6,j_1,j_2,j_3 は共線である．

［証 明］直線 $\overline{i_1,i_2}$ と $\overline{i_5,i_6}$ との交点は $\{i_1,i_2,\cdots,i_6\}$ が 6 角形であるから，この 6 角形を作る 6 点と異なる．したがっていまこれを j_1 とする．同様にして $\overline{i_1,i_3}$ および $\overline{i_4,i_4}$ と $\overline{i_5,i_6}$ との交点をそれぞれ j_2,j_3 とすると，j_1,j_2,j_3 はすべて異なり，$\{i_5,\ i_6,\ j_1,\ j_2,\ j_3\}=\overline{i_5,i_6}$ である．いま $\overline{i_3,i_4}\cap\overline{i_5,i_6}=j_1'$ とすると j_1' は j_1,j_2 または j_3 に一致する．ここで $\overline{i_3,i_4}$ は $\overline{i_1,i_3}$，$\overline{i_1,i_4}$ とそれぞれ i_3,i_4 で交わるから，$j_1'\neq j_2,j_3$ となり $j_1'=j_1$ である．同様にして $\overline{i_2,i_4}$ は j_2 を $\overline{i_2,i_3}$ は j_3 を通り $\{i_1,i_2,i_3,i_4,j_1,j_2,j_3\}$ は 7 角形を作る．



3-6 図

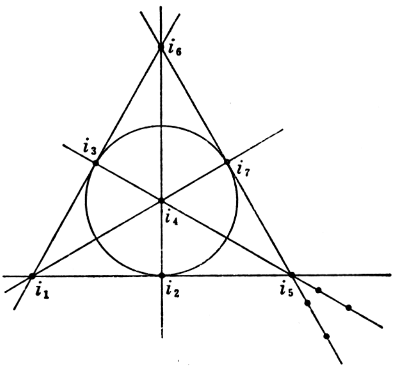
さらに $\{i_1,i_2,i_3,i_4\}$ を含む 7 角形は $\overline{i_1,i_2}\cap\overline{i_3,i_4}=j_1$，$\overline{i_1,i_3}\cap\overline{i_2,i_4}=j_2$，$\overline{i_1,i_4}\cap\overline{i_2,i_3}$

$=j_3$ を含むから，ただ1つである．□

（X）　$\{i_1, i_2, \cdots, i_7\}$ を7角形とすると，この7角形と4点を共有する6角形はすべて同じ K-軌道に含まれる．したがって7角形全体の集合の上でKは3個の軌道 $\overline{\mathfrak{C}}_1, \overline{\mathfrak{C}}_2, \overline{\mathfrak{C}}_3$ を作る．ここで$\overline{\mathfrak{C}}_i (i=1,2,3)$ の7角形と4点を共有する6角形はすべて $\mathfrak{C}_i$ の元で，$|\overline{\mathfrak{C}}_i|=120$ である．

$\overline{\mathfrak{C}}_1, \overline{\mathfrak{C}}_2, \overline{\mathfrak{C}}_3$ を7角形類ということにする．

［証 明］　7角形の異なる2つの4角形は少なくとも1点を共有するから，$\{i_1, i_2, i_3, i_4\}$，$\{i_1, i_2', i_3', i_4'\}$ を異なる2つの4角形とする．4角形 $\{i_1, i_2, i_3, i_4\}$ に対して7角形の残りの3点 i_5, i_6, i_7 は（IX）より共線である．したがって $\{i_2', i_3', i_4'\} \neq \{i_5, i_6, i_7\}$ となり，この2つの4角形は2点または3点を共有する．さらに共線でない3点 i_1, i_2, i_3 に対して3直線 $\overline{i_1, i_2}$，$\overline{i_1, i_3}$，$\overline{i_2, i_3}$ 上に7角形の6点が存在するから，3点 i_1, i_2, i_3 により4角形 $\{i_1, i_2, i_3, i_4\}$ が一意的に決まる．これより異なる4角形はちょうど2点を共有する．したがって $\{i_1, i_2', i_3', i_4'\}=\{i_1, i_2, i_3', i_4'\}$ としてよい．さらに $\overline{i_1, i_2}$ 上に i_5 があるとすると $\{i_1, i_2, i_3', i_4'\}=\{i_1, i_2, i_6, i_7\}$ である．4角形 $\{i_1, i_2, i_3, i_4\{$ を含む6角形の残りの2点は(IX)より，$\overline{i_6, i_7}$ 上にあり，4角形 $\{i_1, i_2, i_6, i_7\}$ を含む6角形の残りの2点は $\overline{i_3, i_4}$ 上にあるから，これら2つの6角形の共有点は i_1, i_2 のみとなり（VIII）より同じ K-軌道に含まれる．



逆にCを6角形とし，$\bar{C}, \bar{C}'$ を $|C\cap\bar{C}|=|C\cap\bar{C}'|=4$ である7角形とする．（VI）の証明で示したようにKのCへの制限 K^C は交代群 A_6 であるから $K_{(C)}$ に $C\cap\bar{C}$ を $C\cap\bar{C}'$ にうつす元が存在し，（IX）よりこの元は $\bar{C}$ を $\bar{C}'$ にうつす．すなわち $\bar{C}$ と $\bar{C}'$ は同じ K-軌道に属する．

以上より6角形の集合の上の K-軌道 $\mathfrak{C}_1$，$\mathfrak{C}_2$，$\mathfrak{C}_3$ に対して，$\overline{\mathfrak{C}}_i$ $(i=1,2,3)$ を $|\bar{C}\cap C|=4$ なる $C\in\mathfrak{C}_i$ が存在する7角形 $\bar{C}$ の集合とすると，$\overline{\mathfrak{C}}_1$，$\overline{\mathfrak{C}}_2$，$\overline{\mathfrak{C}}_3$ は7角形の集合の上の K- 軌道である．

7角形に含まれる4角形は，7角形の任意の2点に対してこれを含む4角形が2個存在するから $\binom{7}{2}\cdot 2\Big/\binom{4}{2}=7$ 個存在する．一方6角形に含まれる4角形は $\binom{6}{4}=15$

個存在し，(IX) より 15 個の 4 角形は異なる 7 角形をそれぞれ一意的に決める．したがって $|\mathfrak{C}_i|=56$ より $|\overline{\mathfrak{C}_i}|=56\cdot15/7=120$ である．□

以下 W_{22}, W_{23}, W_{24} と同じパラメーターをもつデザインは同型であることを示すが，その方法は前節の方法とほとんど同じである．

補 題 5.2 $D=(\Omega,\mathfrak{B})$ を 3-(22, 6, 1)デザイン，$p\in\Omega$, $\mathfrak{C}=\{C\in\mathfrak{B}\mid p\notin C\}$ とする．このとき D_p は位数 4 の射影平面で $\mathfrak{C}$ は D_p の 6 角形類の 1 つに一致する．

［証 明］ D_p は 2-(21, 5, 1) デザインであるから位数 4 の射影平面であり，その 6 角形類を $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$ とする．$\mathfrak{C}$ のブロックは，D_p においていずれの 3 点も共線でない 6 点の集合，すなわち D_p の 6 角形よりなる．定理 2.8 より $|\mathfrak{B}|=\dfrac{22\cdot21\cdot20}{6\cdot5\cdot4}=77$, p を通るブロックは $\dfrac{21\cdot20}{5\cdot4}=21$ 個であるから $|\mathfrak{C}|=77-21=56$ である．また D_p の 2 点に対して，この 2 点を含む D のブロックは $\dfrac{20}{4}=5$ 個で，そのうち 1 個は p を含むブロックであるから，$\mathfrak{C}$ の元はちょうど 4 個で D は会合数 1 の 3- デザインだからこの 4 個のブロックのいずれの 2 つのブロックもこの 2 点以外に共有点をもたない．

$C=\{p_1,p_2,\cdots,p_6\}$ を $\mathfrak{C}$ の元とし，$C\in\mathfrak{C}_1$ とする．C の任意の 2 点に対して C とこの 2 点のみを共有する D_p の 6 角形は補題 5.1 (VIII) より 3 個存在し，上に述べたように 3 個とも $\mathfrak{C}$ の元である．さらに C と 2 点を共有するから補題 5.1 (VII) より C と同じ 6 角形類 $\mathfrak{C}_1$ の元である．したがって C と 2 点のみを共有する D_p の 6 角形は $\binom{6}{2}\cdot3=45$ 個存在し，C と共に 46 個の $\mathfrak{C}_1$ の元が $\mathfrak{C}$ に含まれる．

いま $C'\in\mathfrak{C}_i$ $(i\neq1)$ が $\mathfrak{C}$ に含まれると同様にして 46 個の $\mathfrak{C}_i$ の元が $\mathfrak{C}$ に属する．ここで $\mathfrak{C}_1\cap\mathfrak{C}_i=\phi$ であるから $46+46\leqq|\mathfrak{C}|$ となり $|\mathfrak{C}|=56$ に反する．したがって $\mathfrak{C}=\mathfrak{C}_1$ である．□

定 理 5.3 3-(22, 6, 1) デザインは W_{22} に同型である．

［証 明］ 定理 2.7 より W_{22} は 3-(22, 6, 1) デザインである．いま $D=(\Omega,\mathfrak{B})$, $D'=(\Omega',\mathfrak{B}')$ を任意の 3-(22, 6, 1) デザインとし $p\in\Omega$, $p'\in\Omega'$ とする．

$\mathfrak{B}_0=\{B\in\mathfrak{B}\mid p\notin B\}$, $\mathfrak{B}_0'=\{B'\in\mathfrak{B}'\mid p'\notin B'\}$ とおく．D_p, $D'_{p'}$ は系 3.17 より同型な位数 4 の射影平面で，補題 5.2 より $\mathfrak{B}_0$, $\mathfrak{B}_0'$ はそれぞれ D_p, $D'_{p'}$ の 1 つの 6 角形類である．さらに補題 5.1 (VII) より $\mathrm{Aut}\,D'_{p'}$ は $D'_{p'}$ の 6 角形類の集合の上に可移に作用する．したがって定理 4.4 の証明と同様にして D と D' は同型である．□

定 理 5.4 4-(23, 7, 1) デザインは W_{23} に同型である．

［証 明］ 定理 2.7 より W_{23} は 4-(23,7,1) デザインである.

$D=(\Omega, \mathfrak{B})$ を 4-(23,7,1) デザイン, p, $q(\neq)\in\Omega$ とする. このとき D_p, D_q は 3-(22,6,1) デザイン, $D_{p,q}$ は位数 4 の射影平面である. $D_{p,q}$ において, 6 角形類を $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$, それに対応する 7 角形類を $\overline{\mathfrak{C}_1}$, $\overline{\mathfrak{C}_2}$, $\overline{\mathfrak{C}_3}$ とする. 補題 2.8 より $|\mathfrak{B}|=\dfrac{23\cdot22\cdot21\cdot20}{7\cdot6\cdot5\cdot4}=253$ で $\mathfrak{B}$ は次のブロックよりなる.

（i） $\{p,q\}$ と $D_{p,q}$ の直線よりなる 21 個のブロック.

（ii） $\{p\}$ と $D_{p,q}$ の 1 つの 6 角形類（$\mathfrak{C}_1$ とする）の 6 角形よりなる 56 個のブロック.

（iii） $\{q\}$ と $D_{p,q}$ の $\mathfrak{C}_1$ と異なる 1 つの 6 角形類（$\mathfrak{C}_2$ とする）の 6 角形よりなる 56個のブロック.

（iv） $D_{p,q}$ の 7 点よりなるブロックで, このブロックの集合を $\overline{\mathfrak{C}}$ とおくとき, $|\overline{\mathfrak{C}}|=253-21-56-56=120$ である.

$B=\{p_1,p_2,\cdots,p_7\}\in\overline{\mathfrak{C}}$ とし, 任意の $p_i,p_j\,(\neq)\in B$ をとる. p,q,p_i,p_j を通るブロック $B'\in\mathfrak{B}$ がただ 1 つ存在し, B' は $\{p,q\}$ と $D_{p,q}$ の p_i,p_j を通る直線よりなる. 一方 B,B' は共に p_i,p_j を含むから, B,B' は $\{p_i,p_j\}$ と位数 4 の射影平面 D_{p_i,p_j} の直線からなり, したがって B と B' は D_{p_i,p_j} 上に共有点をただ 1 つもつ. すなわち p_i, p_j を通る $D_{p,q}$ の直線は B と 3 点を共有する. これより B は 2-(7,3,1) デザインとなり $D_{p,q}$ の 7 角形である. さらに B に含まれる 4 角形は (ii), (iii) より $\mathfrak{C}_1$, $\mathfrak{C}_2$ の 6 角形に含まれない. すなわち B に含まれる 4 角形は $\mathfrak{C}_3$ の 6 角形を作り, 補題 5.1(X) より $B\in\overline{\mathfrak{C}_3}$ である. したがって $\overline{\mathfrak{C}}\subseteqq\overline{\mathfrak{C}_3}$ で補題 5.1 (X) より $|\overline{\mathfrak{C}_3}|=120$ であるから, $\overline{\mathfrak{C}}=\overline{\mathfrak{C}_3}$ である.

$D=(\Omega, \mathfrak{B}), D'=(\Omega', \mathfrak{B}')$ を任意の 4-(23,7,1) デザインとし, $p\in\Omega, p'\in\Omega'$ とする. D_p, $D'_{p'}$ は共に 3-(22,6,1) デザインで定理 5.3 より同型である. いま D_p から $D'_{p'}$ への同型を φ とし, $q\in\Omega-\{p\}$ に対して $q^\varphi=q'$ とする. また $\mathfrak{B}_0=\{B\in\mathfrak{B}\,|\,p\notin B\}$, $\mathfrak{B}_0'=\{B'\in\mathfrak{B}'\,|\,p'\notin B'\}$, $D_{p,q}$ の 6 角形類を $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$, $D'_{p',q'}$ の 6 角形類を $\mathfrak{C}_1'$, $\mathfrak{C}_2'$, $\mathfrak{C}_3'$ とする. このとき D_p の q を含まないブロックの集合を $\mathfrak{C}_1$, $D'_{p'}$ の q' を含まないブロックの集合を $\mathfrak{C}_1'$ とすると

$$\mathfrak{B}_0=\{\{q\}\cup C\,|\,C\in\mathfrak{C}_2\}\cup\overline{\mathfrak{C}_3},$$

$$\mathfrak{B}_0'=\{\{q'\}\cup C'\,|\,C'\in\mathfrak{C}_2'\}\cup\overline{\mathfrak{C}_3'}$$

となり, 定理 4.5 の証明と同様にして D と D' は同型となる. □

定 理 5.5 5-(24,8,1) デザインは W_{24} に同型である.

［証 明］ 定理2.7より W_{24} は 5-(24, 8, 1) デザインである．

$D=(\Omega,\ \mathfrak{B})$ を 5-(24, 8, 1) デザイン，$p, q, r(\neq)\in\Omega$ とする．$D_{p,q,r}$ は位数4の射影平面でその6角形類を $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$, 7角形類を $\bar{\mathfrak{C}}_1$, $\bar{\mathfrak{C}}_2$, $\bar{\mathfrak{C}}_3$ とする．補題2.8より $|\mathfrak{B}|=\dfrac{24\cdot23\cdot22\cdot21\cdot20}{8\cdot7\cdot6\cdot5\cdot4}=759$ でこのうち p を含むブロックは $\dfrac{23\cdot22\cdot21\cdot20}{7\cdot6\cdot5\cdot4}=$ 253 個で，$\{p\}$ と D_p のブロックの和集合である．したがって定理5.4で示したように

$$\{\{p,q,r\}\cup l\,|\,l \text{ は } D_{p,q,r} \text{ の直線}\}$$
$$\cup\{\{p,q\}\cup C\,|\,C \text{ は } D_{p,q,r} \text{ の6角形類} \mathfrak{C}_1 \text{ の6角形}\}$$
$$\cup\{\{p,r\}\cup C\,|\,C \text{ は } D_{p,q,r} \text{ の6角形類} \mathfrak{C}_2 \text{ の6角形}\}$$
$$\cup\{\{p\}\cup \bar{C}\,|\,\bar{C} \text{ は } D_{p,q,r} \text{ の7角形類} \bar{\mathfrak{C}}_3 \text{ の7角形}\}$$

である．いま $D_{p,q,r}$ の2つの7角形 $\bar{C},\bar{C}'$ が $|\bar{C}\cap\bar{C}'|\geqq5$ であれば明らかに $\bar{C}=\bar{C}'$ である．したがって $\bar{C},\bar{C}'$ が異なるとき共有点は高々4個である．これより p を含まないブロックは $759-253=506$ 個存在し

$$\{\{q,r\}\cup C\,|\,C \text{ は } D_{p,q,r} \text{ の6角形類} \mathfrak{C}_3 \text{ の6角形}\}$$
$$\cup\{\{q\}\cup \bar{C}\,|\,\bar{C} \text{ は } D_{p,q,r} \text{ の7角形類} \bar{\mathfrak{C}}_2 \text{ の7角形}\}$$
$$\cup\{\{r\}\cup \bar{C}\,|\,\bar{C} \text{ は } D_{p,q,r} \text{ の7角形類} \bar{\mathfrak{C}}_1 \text{ の7角形}\}$$
$$\cup\{D_{p,q,r} \text{ の8点よりなる} D \text{ のブロック}\}$$

である．ここで D のブロックを作る $D_{p,q,r}$ の8点を8角形，その集合を8角形類とよぶと，8角形類は $506-56-120-120=210$ 個の8角形よりなる．また p を含まない D のブロックは上に示したように，8角形類を除き p を含む D のブロックにより一意的に定まる．

$\{p_1, p_2, \cdots, p_8\}$ を8角形とする．$\{p_1, p_2, \cdots, p_8\}$ は $D_{p,q,r}$ の6角形を含まないから，共線である3点が存在しこれを p_1, p_2, p_3 とする．すると $\{p, q, r\}\cup\overline{p_1, p_2}$ は D のブロックで $\{p_1, p_2, p_3\}$ を含む．したがって D_{p_1,p_2,p_3} において $\{p_4, p_5, \cdots, p_8\}$ と $\{p, q, r\}$ は異なる直線に含まれ，D_{p_1,p_2,p_3} は射影平面であるからこの2直線は交わり，その交点を p_4 としてよい．すなわち $\{p, q, r, p_1, p_2, p_3, p_4\}$ は D のブロックに含まれしたがって $D_{p,q,r}$ において p_1, p_2, p_3, p_4 は共線である．さらにこのことより $\{p_1,\ p_2, \cdots,\ p_8\}$ において，3点が共線であればこの3点を含む $\{p_1, p_2, \cdots, p_8\}$ の4点が共線である．

いま p_5, p_6, p_7, p_8 が4角形を作るとする．このとき $\{p_5, p_6, p_7, p_8\}$ を含む6角形に含まれない $p_i\in\{p_1, p_2, p_3, p_4\}$ が存在し，p_i, p_5, p_6 は共線であるとしてよい．すると上に述べたことより $p_j\in\{p_1, p_2, p_3, p_4\}-\{p_i\}$ がこの直線上にあり，$\overline{p_1, p_2}=\overline{p_i, p_j}=\overline{p_5, p_6}$ となり，$\overline{p_1, p_2}$ に6点 $p_1, p_2, \cdots, p_6$ が存在して $|\overline{p_1, p_2}|=5$ に反する．したがって p_5,

p_6, p_7 は共線であるとしてよい．さらに $p_8 \in \overline{p_1, p_2}$ とするとDのブロック $\{p, q, r, p_1, p_2, p_3, p_4, p_8\}$ と８角形 $\{p_1, p_2, \cdots, p_8\}$ がちょうど５点を共有し，D が会合数１の 5-デザインであることに反する．したがって $p_8 \notin \overline{p_1, p_2}$ である．また p_8 を通る直線は５個だから $\overline{p_8, p_i}$ $(i=1,2,\cdots,7)$ のうち一致するものが存在する．すなわち p_8 を含む３点が共線になり，したがって p_8 を含む４点が共線となり，この直線は $\overline{p_1, p_2}$ にならないから，p_5, p_6, p_7, p_8 が共線となる．また，上に述べたように $\{p_1, p_2, \cdots, p_8\}$ の５点が共線にはならないから，$p_1, p_2, \cdots, p_8$ は２直線 $\overline{p_1, p_2}$ と $\overline{p_5, p_6}$ 上の交点を除く８点である．

$D_{p,q,r}$ において２直線の組は $\binom{21}{2}=210$ 個であるから，これら全体により８角形類が作られ，このことより p, q, r を含まないDのブロックは $D_{p,q,r}$ において一意的に定まる．

$D=(\Omega, \mathfrak{B})$, $D'=(\Omega', \mathfrak{B}')$ を任意の 5-(24, 8, 1) デザインとするとき，以上の結果を用いて，定理 4.6 の証明と同じようにして，DとD'は同型であることが証明される．□

定理 5.6 $\mathrm{Aut}\, W_{24}=M_{24}$, $\mathrm{Aut}\, W_{23}=M_{23}$, $\mathrm{Aut}\, W_{22}=\bar{M}_{22}$ である．ここで $\bar{M}_{22}=N_{M_{24}}(M_{22})$で $|\bar{M}_{22}:M_{22}|=2$ である．

［証 明］（i） $D=W_{22}, G=\mathrm{Aut}\ W_{22}$ とおく．D は W_{24} の２点の内部構造であるから，定理 2.7 より $\bar{M}_{22}=N_{M_{24}}(M_{22}) \leqq G$ である．したがって $|G| \geqq |\bar{M}_{22}|=2 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ である．

Dの点pに対してD_pは位数４の影射平面 $PG(2,4)$ であるから，定理 3.9 によって $\mathrm{Aut}\, D_p=P\Gamma L(3,4)$ で $|\mathrm{Aut}\, D_p|=2 \cdot \dfrac{(4^3-1)(4^3-4)(4^3-4^2)}{4-1}=6 \cdot 21 \cdot 20 \cdot 48$ である．D_p の６角形類を $\mathfrak{C}_1, \mathfrak{C}_2\ \mathfrak{C}_3$ とすると補題 5.2 より p を含まないDのブロックの集合を $\mathfrak{C}_1$ としてよい．$\mathrm{Aut}\, D_p$ は $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ に作用し，補題 5.1 (VII) よりこの上で対称群 S_3 である．したがって $\mathrm{Aut}\, D_p$ における $\mathfrak{C}_1$ の安定化群 $(\mathrm{Aut}\, D_p)_{\mathfrak{C}_1}$ は$|(\mathrm{Aut}\ D_p)_{\mathfrak{C}_1}|=|\mathrm{Aut}\ D_p|/3=2 \cdot 21 \cdot 20 \cdot 48$ である．

一方Gにおける点pの安定化群 G_p は D_p 上 $(\mathrm{Aut}\, D_p)_{\mathfrak{C}_1}$ の部分群であるから，$|G_p| \leqq |(\mathrm{Aut}\, D_p)_{\mathfrak{C}_1}|$ となり，さらに G は D の点集合上可移であるから，$|G|=22 \cdot |G_p| \leqq 22 \cdot 2 \cdot 21 \cdot 20 \cdot 48$ である．したがって $|G|=|\bar{M}_{22}|, G=\bar{M}_{22}$ となる．

（ii） $D=W_{23}$, $G=\mathrm{Aut}\, D$ とおくと $G \geqq M_{23}$ で，したがって $|G| \geqq |M_{23}|=23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ である．いま $p, q(\neq)$ をDの２点とする．$D_{p,q}$ は $PG(2,4)$ であるから $|\mathrm{Aut}\ D_{p,q}|=|P\Gamma L(3,4)|=6 \cdot 21 \cdot 20 \cdot 48$ で $G_{p\,q}$ は $D_{p,q}$ 上 $\mathrm{Aut}\ D_{p,q}$

の部分群である．ここで $D_{p,q}$ の6角形類を $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ とすると，Aut $D_{p,q}$ は $\{\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3\}$ 上対称群 S_3 であり，定理 5.4 の証明でみたように G_{pq} は $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ を固定する．したがって $|G_{p\,q}| \leqq |\mathrm{Aut}\, D_{p,q}|/6 = 21 \cdot 20 \cdot 48$ である．以上よりGはDの点集合上4重可移であるから，$|G| = 23 \cdot 22 \cdot |G_{p\,q}| \leqq 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = |M_{23}|$ となり $G = M_{23}$ である．

(iii) $D = W_{24}$, $G = \mathrm{Aut}\ D$ とおくと $G \geqq M_{24}$ である．pをDの点とすると(ii)より D_p 上 $G_p \leqq \mathrm{Aut}\ D_p = M_{23}$ である．したがって M_{24} は M_{23} の可移拡大であることより $G = M_{24}$ である．□

補題 5.7 $D = (\Omega, \mathfrak{B})$ を W_{24} とする．

(1) $B_1, B_2 (\neq) \in \mathfrak{B}$ に対して $|B_1 \cap B_2| = 0, 2$ または4である．

(2) $B_1, B_2 \in \mathfrak{B}$ で $|B_1 \cap B_2| = 4$ とすると，$(B_1 \cup B_2) - (B_1 \cap B_2)$ も $\mathfrak{B}$ のブロックである．

(3) $B \in \mathfrak{B}$ の2点 $p_1, p_2 (\neq)$ に対して，B とちょうど2点 p_1, p_2 を共有する $\mathfrak{B}$ のブロックは16個である．

［証 明］ (1) $|B_1| = |B_2| = 8$ で$|B_1 \cap B_2| \lneqq 5$ であるから，B_2 に含まれない B_1 の3点 p_1, p_2, p_3 が存在する．定理 5.5 の証明より，$l = B_1 - \{p_1, p_2, p_3\}$ は D_{p_1,p_2,p_3} の直線であり，B_2 は D_{p_1,p_2,p_3} の8角形すなわち D_{p_1,p_2,p_3} の2直線 $g_1, g_2 (\neq)$ により $B_2 = (g_1 \cup g_2) - (g_1 \cap g_2)$ である．

$g_1 \cap g_2 \in l$ とする．$l = g_1$ または g_2 のとき，D_{p_1,p_2,p_3} の直線は5点よりなるから，$|l \cap B_2| = 4$ したがって$|B_1 \cap B_2| = 4$ である．$l \neq g_1, g_2$ のとき，$|l \cap B_2| = 0$ したがって $|B_1 \cap B_2| = 0$ である．

$g_1 \cap g_2 \notin l$ とする．g_1, g_2 はそれぞれ l とちょうど1点で交わるから，$|l \cap B_2| = 2$ したがって $|B_1 \cap B_2| = 2$ である．

(2) $B_1 \cap B_2 = \{p_1, p_2, p_3, p_4\}$ とする．$l_1 = B_1 - \{p_1, p_2, p_3\}$，$l_2 = B_2 - \{p_1, p_2, p_3\}$ は共に D_{p_1,p_2,p_3} の p_4 を通る直線である．したがって $(B_1 \cup B_2) - (B_1 \cap B_2) = (l_1 \cup l_2) - (l_1 \cap l_2)$ となり，Dの8角形であるから，Dのブロックである．

(3) $p_3, p_4, p_5 (\neq) \in B - \{p_1, p_2\}$ をとる．Bと p_1, p_2 のみを共有するブロックは D_{p_3,p_4,p_5} において，Bと2点 p_1, p_2 のみを共有する8角形である．したがって D_{p_3,p_4,p_5} において $p \notin \overline{p_1, p_2}$ による8角形 $\overline{p, p_1} \cup \overline{p, p_2} - \{p\}$ である．このことより D_{p_3,p_4,p_5} の直線 $\overline{p_1, p_2}$ 上にない点は16個存在するから，Bと p_1, p_2 のみを共有するブロックは16個である．□

補 題 5.8　$D=(\Omega,\mathfrak{B})$ を W_{24} とする．$|B_1\cap B_2|=2$ である $B_1, B_2\in\mathfrak{B}$ をとり，$\Delta=(B_1\cup B_2)-(B_1\cap B_2)$　とおく．

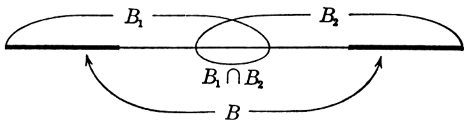
（1）　Δ の任意の 5 点に対してこれを含む $B\in\mathfrak{B}$ をとり，$\bar{B}=\Delta\cap B$ とおくと $|\bar{B}|=6$ である．いま　$\overline{\mathfrak{B}}=\{\bar{B}=\Delta\cap B \mid B\in\mathfrak{B}, |\Delta\cap B|=6\}$　とおくと，結合構造 $(\Delta,\overline{\mathfrak{B}})$ は W_{12} である．

（2）　任意の $\bar{B}\in\overline{\mathfrak{B}}$ $(B\in\mathfrak{B})$ に対して $(\Delta\cup B)-\bar{B}$ は $\mathfrak{B}$のブロックである．

（3）　$\Gamma=\Omega-\Delta$ とおくと　$\Gamma=(B_1'\cup B_2')-(B_1'\cap B_2')$，$|B_1'\cap B_2'|=2$ となる $B_1', B_2'\in\mathfrak{B}$ が存在する．

［証 明］　$|B_1|=|B_2|=8$ で$|B_1\cap B_2|=2$ より $|\Delta|=12$ である．

（1）　いま$B\subset\Delta$とする．補題 5.7 (1) より $|B\cap B_i|=0$, 2 または4 $(i=1,2)$ であるからΔ上で $|B\cap B_1|=|B\cap B_2|=4$ である．したがって補題 5.7 (2) より $B'=(B\cup B_1)-(B\cap B_1)$ は $\mathfrak{B}$ のブロックである．すると $|B'\cap B_2|=6$ となり補題 5.7 (1) に反する．したがってBはΔに含まれない．ここで $|\bar{B}|=|B\cap\Delta|\geqq 5$ であるから，$|\bar{B}|=5, 6$ または7 である．また$|B\cap B_i|$ $(i=1,2)$ は偶数であるから，$|B\cap(B_1\cap B_2)|=0$ または2 であれば $|\bar{B}\cap B_1|$, $|\bar{B}\cap B_2|$ は共に偶数であり，$|B\cap(B_1\cap B_2)|=1$ のとき $|\bar{B}\cap B_1|$, $|\bar{B}\cap B_2|$ は共に奇数である．したがって　$|\bar{B}|=|\bar{B}\cap B_1|+|\bar{B}\cap B_2|$　であるから $|\bar{B}|$ は偶数となり $|\bar{B}|=6$ である．



3-8 図

Δ の任意の 5 点に対して，これを含む $\mathfrak{B}$ のブロックBが一意的に定まり，したがって $\overline{\mathfrak{B}}$ の元 $\bar{B}=B\cap\Delta$ が一意的に定まる．さらに $|\Delta|=12$, $|\bar{B}|=6$ であるから，結合構造 $(\Delta,\overline{\mathfrak{B}})$ は 5-(12, 6, 1) デザインとなり定理 4.6 より，W_{12} である．

（2）　$B_1=\{q_1, q_2, p_1, p_2, \cdots, p_6\}$, $B_2=\{q_1, q_2, p_7, p_8, \cdots, p_{12}\}$, $B_1\cap B_2=\{q_1, q_2\}$, $\Delta=\{p_1, p_2, \cdots, p_{12}\}$ とする．任意の $\bar{B}\in\overline{\mathfrak{B}}$ $(B\in\mathfrak{B})$ に対して $|\bar{B}|=6$ であるから　$|\bar{B}\cap\bar{B}_1|=4$, $|\bar{B}\cap\bar{B}_2|=2$　または　$|\bar{B}\cap\bar{B}_1|=|\bar{B}\cap\bar{B}_2|=3$　としてよい．

いま $|\bar{B}\cap\bar{B}_1|=4$, $|\bar{B}\cap\bar{B}_2|=2$ とする．補題 5.7 (1) より $|B\cap B_1|=4$ となり，したがって　$|B\cap(B_1\cap B_2)|=0$, $|B\cap B_2|=2$　である．すなわち

$$B=\{q_1', q_2', p_1, p_2, p_3, p_4, p_7, p_8\}$$

としてよい．このとき　$B'=(B\cup B_1)-(B\cap B_1)=\{q_1, q_2, q_1', q_2', p_5, p_6, p_7, p_8\}$　は補題 5.7 (2) より$\mathfrak{B}$のブロックである．さらに $B_2\cap B'=\{q_1, q_2, p_7, p_8\}$ であるから同様

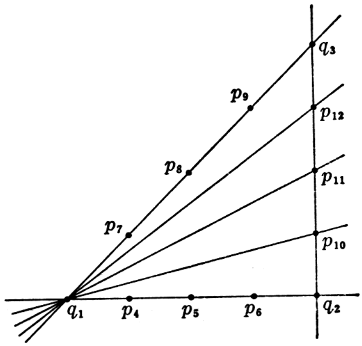
に $B''=(B_2\cup B')-(B_2\cap B')=\{q_1', q_2', p_5, p_6, p_9, p_{10}, p_{11}, p_{12}\}$ は$\mathfrak{B}$のブロックとなり$B''=(\varDelta\cup B)-\bar{B}$ である.

つぎに $|\bar{B}\cap\bar{B}_1|=|\bar{B}\cap\bar{B}_2|=3$ とする. 補題 5.7 (i) より $|B\cap B_1|=|B\cap B_2|=4$ となり

$$B=\{q_1, q_2', p_1, p_2, p_3, p_7, p_8, p_9\}$$

としてよい. このとき上の場合と同様にして, $B'=(B\cup B_1)-(B\cap B_1)=\{q_2, q_2', p_4, p_5, \cdots, p_9\}$ は$\mathfrak{B}$のブロックで, $B'\cap B_2=\{q_2, p_7, p_8, p_9\}$ より, $B''=(B'\cup B_2)-(B'\cap B_2)=\{q_1, q_2', p_4, p_5, p_6, p_{10}, p_{11}, p_{12}\}$ は$\mathfrak{B}$のブロックとなり, $B''=(B\cup\varDelta)-\bar{B}$ である.

(3) (2) のように $B_1=\{q_1, q_2, p_1, p_2, \cdots, p_6\}$, $B_2=\{q_1, q_2, p_7, p_8, \cdots, p_{12}\}$, $\varDelta=\{p_1, p_2, \cdots, p_{12}\}$ とする. D_{p_1,p_2,p_3} において B_1 より $\overline{q_1, q_2}=\{q_1, q_2, p_4, p_5, p_6\}$ であり, 補題 5.7 (1) の証明でみたように D_{p_1,p_2,p_3} に点 q_3 が存在して, $B_2=(\overline{q_1, q_3}\cup\overline{q_2, q_3})-\{q_3\}$ である. したがって $\overline{q_1, q_3}=\{q_1, q_3, p_7, p_8, p_9\}$, $\overline{q_2, q_3}=\{q_2, q_3, p_{10}, p_{11}, p_{12}\}$ としてよい. このとき D_{p_1,p_2,p_3} において $B_1'=(\overline{q_1, p_{10}}\cup\overline{q_1, p_{11}})-\{q_1\}$, $B_2'=(\overline{p_{12}, q_1}\cup\overline{p_{12}, q_2})-\{p_{12}\}$



3-9 図

とおくと, $B_1', B_2'\in\mathfrak{B}$ である. さらに $B_1'\cap\varDelta=B_2'\cap\varDelta=B_1'\cap B_2'=\{p_{10}, p_{11}\}$ であるから, $\varOmega-\varDelta=(B_1'\cup B_2')-(B_1'\cap B_2')$ である. □

定理 5.9 $D=(\varOmega, \mathfrak{B})$ を W_{24}, $G=\mathrm{Aut}\,D=M_{24}$, B_1, B_2 を $|B_1\cap B_2|=2$ である$\mathfrak{B}$のブロック, $\varDelta=(B_1\cup B_2)-(B_1\cap B_2)$, $\varGamma=\varOmega-\varDelta$ とおく.

(1) $G_{(\varDelta)}$ は$\varOmega$上長さ 12 の 2 つの軌道 $\varDelta, \varGamma$ をもち, $G^{\varDelta}$, $G^{\varGamma}$ は共に M_{12} である.

(2) 任意の $p\in\varDelta$ に対して, $H=(G_{(\varDelta)})_p$ とおくとき, H は $\varOmega-\{p\}$ 上長さ11の軌道 $\varDelta-\{p\}$ と長さ 12 の軌道$\varGamma$をもち, $H^{\varDelta-\{p\}}$, $H^{\varGamma}$ は共に M_{11} に同型で, $H^{\varGamma}$ は $\varGamma$ 上ちょうど 3 重可移である.

[証明] (1) $\overline{\mathfrak{B}}=\{\bar{B}=B\cap\varDelta\,|\,B\in\mathfrak{B}, |B\cap\varDelta|=6\}$ とおくと, 補題 5.8 (1) より, 結合構造 $(\varDelta, \overline{\mathfrak{B}})$ は W_{12} である. ここで$\overline{\mathfrak{B}}$は$\mathfrak{B}$より作られたものであるから $G_{(\varDelta)}\leqq\mathrm{Aut}\,(\varDelta, \overline{\mathfrak{B}})$ で, したがって定理 4.7 より $G_{(\varDelta)}\leqq\mathrm{Aut}\,(\varDelta, \overline{\mathfrak{B}})=M_{12}$ である.

Δの任意の異なる4点 p_1, p_2, p_3, p_4 をとる．任意の $p, p' \in \Delta - \{p_1, p_2, p_3, p_4\}$ に対してGはΩ上5重可移であるから，$p^a = p'$ である $a \in G_{p_1p_2p_3p_4}$ が存在する．Dは会合数1の5-デザインであるから，$\{p_1, p_2, p_3, p_4, p\} \subset B_1 \in \mathfrak{B}$, $\{p_1, p_2, p_3, p_4, p'\} \subset B_2 \in \mathfrak{B}$ となるブロック B_1, B_2 が一意的に決まる．このとき補題 5.8 (1) より $|B_1 \cap \Delta| = |B_2 \cap \Delta| = 6$ である．したがって $\bar{B}_1 = B_1 \cap \Delta = \{p_1, p_2, p_3, p_4, p, q\}$, $\bar{B}_2 = B_2 \cap \Delta = \{p_1, p_2, p_3, p_4, p', q'\}$ とおく．$\{p_1, p_2, p_3, p_4, p\}^a = \{p_1, p_2, p_3, p_4, p'\}$ であるから $B_1{}^a = B_2$ となり $q'' = q^a \in B_2$ である．

定理 2.7 および補題 1.7 (2) より G_{B_2} は $G_{p_1p_2p_3p_4p'}$ の2-シロー部分群で $F(G_{B_2}) = B_2$ となり $\Omega - B_2$ 上可移である．さらに系1.9より $G^{B_2} = A_8$ である．したがって $q''^{a'} = q'$ となる元 $a' \in (G_{(B_2)})_{p_1p_2p_3p_4p'}$ が存在する．これより $B_1{}^{aa'} = B_2, p^{aa'} = p'$, $q^{aa'} = q', aa' \in G_{p_1p_2p_3p_4}$ である．いま $\Delta^{aa'} = \Delta'$ とおくと，$B_2 \cap \Delta' = B_2 \cap \Delta = \bar{B}_2$ である．

補題 5.8 (2) より $B_3 = (\Delta \cup B_2) - \bar{B}_2, B_3' = (\Delta' \cup B_2) - \bar{B}_2$ は$\mathfrak{B}$のブロックで $\Delta = (B_2 \cup B_3) - (B_2 \cap B_3), \Delta' = (B_2 \cup B_3') - (B_2 \cap B_3'), B_2 \cap B_3 = B_2 \cap B_3' = B_2 - \bar{B}_2$ である．さらに補題 5.7 (3) の証明で示したように，B_3, B_3' は共に B_2 との共有点が $B_2 - \bar{B}_2$ の2点であるから，$B_2 - \bar{B}_2$ の2点と D_{p_1,p_2,p_3} の1点により一意的に定まる D_{p_1,p_2,p_3} の8角形である．ここで G_{B_2} は $\Omega - B_2$ 上可移であるから $B_3'^b = B_3$ となる $b \in G_{B_2}$ が存在し，これより $\Delta'^b = \Delta$ となる．

以上より $aa'b \in (G_{(\Delta)})_{p_1p_2p_3p_4}$ で $p^{aa'b} = p$ である．すなわちΔの任意の異なる4点 p_1, p_2, p_3, p_4 に対して G^Δ は $\Delta - \{p_1, p_2, p_3, p_4\}$ 上可移となり，したがって G^Δ はΔ上5重可移となる．ここで $G^\Delta \leqq M_{12}$ で $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ であるから $G^\Delta = M_{12}$ である．

つぎに $G_{(\Delta)} = G_{(\Gamma)}$ で補題5.8よりΓ上 $(\Delta, \mathfrak{B})$ と同様にして W_{12} が作られるから，$G^\Gamma = M_{12}$ である．

(2) 補題 5.8 (3) より $B, B' \in \mathfrak{B}$ が存在して $|B \cap B'| = 2, \Gamma = (B \cup B') - (B \cap B')$ である．いま $B \cap B' = \{p, q\}$, $\bar{B} = B \cap \Gamma$, $\bar{B}' = B' \cap \Gamma$ とおく．(1) で示した様に $G^B = A_8$ であるから $G^{\bar{B}} = S_6$ で，補題 1.7 より $G_{(\bar{B})}$ は $\{p, q\}$ を固定し，$|G_{(\bar{B})}| = |S_6| \cdot 16$ である．さらに補題 5.7 (3) よりBとちょうど2点p, qを共有するブロックは16 個存在し，G_B は $\Omega - B$ 上可移であるから，G_B はこの 16 個のブロックの集合上可移である．したがって $G_B \leqq G_{(\bar{B})} \leqq G_{(B)}$ で $G_{(\bar{B})}$ は $\{p, q\}$ を固定するから，これら 16個のブロックの集合上可移である．B' はこのブロックの集合に含まれるから，

$|(G_{(\bar{B})})_{(\bar{B}')}|=|S_6|$ となり，したがって $(G_{(\bar{B})})_{(\bar{B}')}$ は $\bar{B}$, $\bar{B}'$ 上共に S_6 になる．さらに $(G_{(\bar{B})})_p$ は $\bar{B}$ 上 A_6 であるから $(G_{(\bar{B})})_{(\bar{B}'),p}$ は $\bar{B}$, $\bar{B}'$ 上 A_6 となる．ここで $\bar{B}\cup\bar{B}'=\Gamma=\Omega-\varDelta$ より $(G_{(\bar{B})})_{(\bar{B}'),p}\leqq(G_{(\varDelta)})_p=H$ で，Hは $\varDelta-\{p\}$ 上可移である．よって任意の $q'\in\varDelta-\{p,q\}$ に対して $q^a=q'$ となる $a\in H$ が存在し，$\bar{B}^a\neq\bar{B},\bar{B}'$ で H は $\bar{B}^a$ 上 A_6 であるから，HはΓ上可移になる．すなわちHは $\Omega-\{p\}$ 上2つの軌道 $\varDelta-\{p\}$ とΓをもち $H_{(\varDelta)}=H_{(\Gamma)}$ である．

（1）より $G^{\varDelta}=M_{12}$ であるから1点pの安定化群として $H^{\varDelta},H^{\Gamma}$ は M_{11} に同型になる．

$|M_{11}|=12\cdot11\cdot10\cdot6$ であるから H^{Γ} は4重可移ではない．任意の $p_1,p_2(\neq)\in\Gamma$ をとる．$(H^{\Gamma})_{p_1}$ は位数 11 の元をもつから，$(H^{\Gamma})_{p_1}$ は $\Gamma-\{p_1\}$ 上可移である．$|(H^{\Gamma})_{p_1p_2}|=10\cdot6$ であるから $(H^{\Gamma})_{p_1p_2}$ は位数5の元xをもつ．$H^{\Gamma}\leqq G^{\Gamma}=M_{12}$ で M_{12} における位数5の元はちょうど2点を固定するからxはちょうど2点 p_1, p_2 を固定し2つの 5- 巡回置換からなる．さらに $(H^{\Gamma})_{p_1p_2}$ は位数3の元yをもち，M_{12} における位数3の元はちょうど3点を固定するから，yは p_1,p_2 ともう1点を固定し3つの 3- 巡回置換からなる．したがって $\langle x,y\rangle$ は $\Gamma-\{p_1,p_2\}$ 上可移となり，$(H^{\Gamma})_{p_1p_2}$ も $\Gamma-\{p_1,p_2\}$ 上可移になる．

以上より H^{Γ} はΓ上ちょうど3重可移である．□

系 5.10　$D=(\Omega,\mathfrak{B})$ を W_{24}, $G=\mathrm{Aut}\ D$, $B_1,B_2\in\mathfrak{B}$ を $|B_1\cap B_2|=2$, $\varDelta=(B_1\cup B_2)-(B_1\cap B_2)$, $\Gamma=\Omega-\varDelta$, $p\in\varDelta$, $H=(G_{(\varDelta)})_p$ とする．いま $|B\cap\Gamma|=6$, $p\in B$ である $B\in\mathfrak{B}$ をとり $\bar{B}=B\cap\Gamma$ とおく．このとき $\bar{\mathfrak{B}}=\{\bar{B}^x\,|\,x\in H\}$ とすると結合構造 $\bar{D}=(\Gamma,\bar{\mathfrak{B}})$ は 3-(12, 6, 2) デザインである．

さらに $q\in\Gamma$ に対して $\bar{D}$ の q に関する内部構造 $\bar{D}_q$ は 2-(11, 5, 2) デザインで，これはアダマール・デザインである．ここで $2\text{-}(4\lambda+3,2\lambda+1,\lambda)$ デザインを**アダマール・デザイン**という．

［**証明**］ Hは位数 $12\cdot11\cdot10\cdot6$ でΓ上3重可移である．したがって定理 2.2 より $\bar{D}=(\Gamma,\bar{\mathfrak{B}})$ は 3-デザインである．ここで $H_{(\bar{B})}\cong A_6$ であるから $|\bar{\mathfrak{B}}|=|H|/|H_{(B)}|=(12\cdot11\cdot10\cdot6)/(6\cdot5\cdot4\cdot3)=22$ で，定理 2.8 より $22=\lambda\cdot\dfrac{12\cdot11\cdot10}{6\cdot5\cdot4}=11\lambda$ となり $\lambda=2$ である．したがって $\bar{D}$ は 3-(12, 6, 2) デザインである．

つぎに定理 2.1 より $\bar{D}_q$ は 2-(11, 5, 2) デザインである．□

系 5.10 において $\bar{B}=\{q_1,q_2,\cdots,q_6\}$ とすると $H_{q_1q_2q_3}$ は位数が6で，$\Gamma-$

$\{q_1, q_2, q_3\}$ 上 $\{q_4, q_5, q_6\}$ を含む軌道は長さが 6 である．したがってこの長さ 6 の軌道の q_4, q_5, q_6 を除く 3 点と q_1, q_2, q_3 が $\overline{\mathfrak{B}}$ のブロックを作る．

さらに $H_q \leqq \mathrm{Aut}\ \bar{D}_q$ であるが，$H_q = \mathrm{Aut}\ \bar{D}_q \cong PSL(2, 11)$ であることが知られている．これは $PSL(2, 11)$ の 11 次の置換表現である．

問　題　解　答

第　2　章

§1. （17ページ）　**問 1.1**　S_4, 1 とつぎの群である．ここで $\{1,2,3,4\}=\{i,j,k,l\}$ とする．位数2の群：$\langle(i\ j)\rangle$ の形で6個，$\langle(i\ j)(k\ l)\rangle$ の形で3個．位数3の群：$\langle(i\ j\ k)\rangle$ の形で4個．位数4の群：$\langle(i\ j\ k\ l)\rangle$ の形で3個，$\langle(1\ 2)(3\ 4),(1\ 3)\cdot(2\ 4)\rangle$．位数6の群：$\{i,j,k\}$ 上対称群 S_3 で3個．位数8の群：$\langle(i\ j\ k\ l),\ (i\ k)\rangle$ の形で3個．位数12の群$\langle(1\ 2\ 3),(1\ 2)(3\ 4)\rangle$．

問 1.2　$G_1=\{a_1=(1\ 2), b_1=(3\ 4), a_1b_1=(1\ 2)(3\ 4), 1\}$，$G_2=\{a_2=(1\ 2)\cdot(3\ 4), b_2=(1\ 3)(2\ 4), a_2b_2=(1\ 4)(2\ 3), 1\}$ で，ともに位数は4である．写像 $G_1\to G_2, a_1\mapsto a_2, b_1\mapsto b_2$ は同型を与える．

問 1.3　$(1\ 2\ 3)=(2\ 3\ 1)=(3\ 1\ 2)$ に注意して，(5) 型：$4!=24$ 個，(4) 型：$\binom{5}{4}\cdot 3!=30$個，(3) 型：$\binom{5}{3}\cdot 2!=20$ 個，(3, 2) 型：$\binom{5}{3}\cdot 2!=20$個，(2) 型：$\binom{5}{2}=10$ 個，(2, 2) 型：$\binom{5}{2}\cdot\binom{3}{2}\cdot\frac{1}{2}=15$ 個，(1) 型：1個　である．

問 1.4　$a^2=(1\ 3)(2\ 4)(5\ 7)(6\ 8)$，$a^3=a^{-1}=(1\ 4\ 3\ 2)(5\ 8\ 7\ 6)$　である．$b^{-1}ab=(1\ 4\ 2\ 3)(5\ 8\ 7\ 6)=a^{-1}$ より $G\triangleright\langle a\rangle$ で，$a^2=b^2$ より $|G|=2\cdot|\langle a\rangle|=8$ となる．Gの元は上記のほかに，$ab=(1\ 8\ 3\ 6)(2\ 7\ 4\ 5)$，$a^{-1}b=(1\ 6\ 3\ 8)\cdot(2\ 5\ 4\ 7)$，$a^2b=b^3=b^{-1}=(1\ 7\ 3\ 5)(2\ 6\ 4\ 8)$　である．

§2. （19ページ）　**問 2.1**　対称群 S_4 と問 1.1 の位数 12の群　$\langle(1\ 2\ 3),(1\ 2)\cdot(3\ 4)\rangle$　の2つである．

問 2.2　問 1.2 の G_1, G_2 は群として同型で，G_2 は $\{1,2,3,4\}$ 上可移であるが，G_1 は可移でない．

問 2.3　文字1をΩの任意の文字に移すGの元が存在するから可移である．$1^x=1$ なる元xは単位元のみであるから2重可移ではない．

問 2.4　$(\lambda_1,\lambda_2)^{a_\alpha a_{\alpha'}}=(\alpha\alpha'\lambda_1,\ (\alpha\alpha')^{-1}\lambda_2)=(\lambda_1,\lambda_2)^{a_{\alpha\alpha'}}$，$(\lambda_1,\lambda_2)^{a_\alpha b_{\alpha'}}=(\alpha\alpha'\lambda_1,\ -(\alpha\alpha')^{-1}\lambda_2)=(\lambda_1,\lambda_2)^{b_{\alpha\alpha'}}$，$(\lambda_1,\lambda_2)^{b_\alpha b_{\alpha'}}=(\alpha\alpha'\lambda_1,(\alpha\alpha')^{-1}\lambda_2)=(\lambda_1,\lambda_2)^{a_{\alpha\alpha'}}$ より，$H=\{a_\alpha, b_\alpha\,|\,\alpha\in GF(q)-\{0\}\}$ は位数 $2(q-1)$ の可換群である．$c^2=1$ で $(\lambda_1,\lambda_2)^{ca_\alpha c}$

$=(\lambda_2, \lambda_1)^{a_\alpha c} = (\alpha\lambda_2, \alpha^{-1}\lambda_1)^c = (\alpha^{-1}\lambda_1, \alpha\lambda_2) = (\lambda_1, \lambda_2)^{a_{\alpha^{-1}}}$.　$(\lambda_1, \lambda_2)^{cb_\alpha c} = (\lambda_2, \lambda_1)^{b_\alpha c} = (\alpha\lambda_2, -\alpha^{-1}\lambda_1)^c = (-\alpha^{-1}\lambda_1, \alpha\lambda_2) = (\lambda_1, \lambda_2)^{b_{-\alpha^{-1}}}$ より $ca_\alpha c = a_{\alpha^{-1}}$, $cb_\alpha c = b_{-\alpha^{-1}}$ となり，$G \triangleright H$ である．したがって $|G| = 4(q-1)$ となる．

$(0,0)^G = \{(0,0)\}$，$\lambda \neq 0$ のとき $(\lambda, 0)^G = \{(\xi, 0), (0, \xi) \mid \xi \in GF(q) - \{0\}\}$，$\lambda_1\lambda_2 \neq 0$ のとき $(\lambda_1, \lambda_2)^G = \{(\xi\lambda_1, \pm\xi^{-1}\lambda_2), (\pm\xi^{-1}\lambda_2, \xi\lambda_1) \mid \xi \in GF(q) - \{0\}\}$，ここで $(\pm\xi^{-1}\lambda_2, \xi\lambda_1) = ((\pm\xi^{-1}\lambda_2\lambda_1^{-1})\lambda_1, (\pm\xi^{-1}\lambda_2\lambda_1^{-1})^{-1}\lambda_2)$ であるから，$(\lambda_1, \lambda_2)^G = \{(\xi\lambda_1, \pm\xi^{-1}\lambda_2) \mid \xi \in GF(q) - \{0\}\}$ となり，V 上の G-軌道は $\{(0,0)\}$ を除き，長さはすべて $2(q-1)$ である．

§ 3. (27ページ)　**問 3.1**　任意の互換 $(i\ j)$ $(i, j \neq 1)$ に対して，$(i\ j) = (1\ i)\cdot(1\ j)(1\ i)$ である．

問 3.2　$a = (1\ 2)$, $b = (2\ 3 \cdots n)$ とすると，$a^{b^i} = (1\ 2+i)$, $i = 1, 2, \cdots, n-2$, である．

問 3.3　$a = (i_1 \cdots i_r)(j_1 \cdots j_s)\cdots(k_1 \cdots k_t)$（長さ1の巡回成分も含む巡回表示）とする．$r$ が偶数のとき $u = (i_1 \cdots i_r)$ は奇置換で $a^u = a$，また $r = s$ が奇数のとき $u = (i_1\ j_1)\cdots(i_r\ j_r)$ は奇置換で $a^u = a$ である．したがって定理 3.8 より C は A_n の共役類である．逆に C を A_n の共役類とすると $a^u = a$ なる奇置換 u が存在する．$a_1 = (i_1 \cdots i_r)$, $a_2 = (j_1 \cdots j_s)$, $\cdots$, $a_m = (k_1 \cdots k_t)$ とおくと $a = a_1a_2\cdots a_m$ で，$a = a^u$ より $a_1{}^u a_2{}^u \cdots a_m{}^u = a_1a_2\cdots a_m$ である．

いま $a_1, a_2, \cdots, a_m$ は異なる奇数の長さとする．このとき $a_1{}^u = a_1, a_2{}^u = a_2, \cdots, a_m{}^u = a_m$ である．$a_1{}^u = (i_1{}^u \cdots i_r{}^u) = (i_1 \cdots i_r)$ より $\{i_1, \cdots, i_r\}^u = \{i_1, \cdots, i_r\}$ である．$i_1{}^u = i_1$ とすると $(i_1\ i_2{}^u \cdots i_r{}^u) = (i_1\ i_2 \cdots i_r)$，したがって $i_2{}^u = i_2, \cdots, i_r{}^u = i_r$ となり u は $\{i_1, \cdots, i_r\}$ 上恒等置換 $a_1{}^r$ である．$i_1{}^u = i_{r'+1} \neq i_1$ とする $a_1{}^{r'}u^{-1}$ は a と可換で $i_1{}^{a_1{}^{r'}u^{-1}} = i_{r'}{}^{u^{-1}} = i_1$，したがって $a_1{}^{r'}u^{-1}$ は $\{i_1, \cdots, i_r\}$ 上1すなわち $a_1{}^{r'} = u$ である．以上より $u = a_1{}^{r'}a_2{}^{s'}\cdots a_m{}^{t'}$ となり u は偶置換となり矛盾である．

問 3.4　高々 t 個の文字のみを動かす元 $(\neq 1)$ が G に存在することを示す．$a\ (\neq 1) \in G$ が $t+1 \leqq k \leqq 2t-3$ なる k 個の文字 $1, 2, \cdots, k$ を動かし残りを固定するとする．$a = (1\ 2 \cdots)\cdots(\cdots\ t-1)(t \cdots)\cdots(\cdots\ k)$ または $a = (1\ 2\cdots)\cdots(\cdots\ t-1\ t \cdots)\cdots(\cdots\ k)$ とする．G は t 重可移だから，$x = \begin{pmatrix} 1 & 2 & \cdots & t-1 & t & t+1 & \cdots & k & \cdots \\ 1 & 2 & \cdots & t-1 & t+1 & (t+1)' & \cdots & k' & \cdots \end{pmatrix}$ が G に存在し，$a^x = (1\ 2 \cdots)\cdots(\cdots\ t-1)(t+1 \cdots)\cdots(\cdots\ k')$ または $a^x = (1\ 2 \cdots)\cdots(\cdots\ t-1\ t+1 \cdots)\cdots(\cdots\ k')$ である．したがって a^xa^{-1} は $\{t, t+1, \cdots, k, (t+1)', \cdots, k'\}$ の $k-(t-1)+k-t = 2k-2t+1$ 個　または $\{t-1, \cdots, k,$

$(t+1)', \cdots, k'\}$ の $2k-2t+2$ 個の文字を高々動かす．

仮定より $2k-2t+2 \leqq 2k-k-3+2=k-1<k$ となり，さらに $a^x a^{-1}$ をまた a として順次 $a^x a^{-1}$ を作ることにより，$k \leqq t$ なる k 個の文字を動かす元 a が存在する．$k=2$ のとき，明らかに $G=S_n$ である．$k \geqq 3$ とする．このとき $a=(i_1\, i_2 \cdots)\cdots(\cdots\, i_{k-1}\ i_k)(i_{k+1})\cdots(i_n)$ で G の元 $x=\begin{pmatrix} i_1 & \cdots & i_{k-1} & i_k & i_{k+1} & \cdots \\ i_1 & \cdots & i_{k-1} & i_{k+1} & i'_{k+1} & \cdots \end{pmatrix}$ により，$a^x=(i_1\ i_2 \cdots)(\cdots\ i_{k-1}\ i_{k+1})(i_k)\cdots(i'_n)$，$a^x a^{-1}=(i_{k-1}\ i_k\ i_{k+1})$ となり，補題 3.10 より $G \geqq A_n$ である．

§ **4**. (32 ページ)　**問 4.1**　x, y を正 n 面体の回転である任意の置換とすると，xy は回転を 2 回続けたものであるから，やはり正 n 面体の回転となり，したがってこれらの置換は群を作る．

（1）　正 4 面体群を G とする．$a=(1\ 2\ 3)$，$b=(1\,3\,4)$，(2－1 図参照) は G の元で，$\langle a, b\rangle$ は $\{1,2,3,4\}$ 上可移である．また $a \in G_1$ で $G_{1\,2}=1$ より，$G_1=\langle a\rangle$，したがって G は $\{1,2,3,4\}$ 上 2 重可移で，$G=A_4$ である．

（2）　正 6 面体群を G とする．$a=(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$，$b=(2\ 5\ 4)(3\ 6\ 8)$，(2－2 図参照) は G の元で，$\langle a, b\rangle$ は $\{1,2,\cdots,8\}$ 上可移である．また $b \in G_1$ で $G_{1\,2}=1$ より，$G_1=\langle b\rangle$ である．したがって G_1 の軌道は $\{1\}$，$\{7\}$，$\{2,4,5\}$，$\{3,6,8\}$ となり，$|G|=8\cdot|G_1|=24$ で階数は 4 である．

つぎに $x \in G$ は，$\{l_1, l_2, l_3, l_4\}$ の置換を導くことは明らかである．したがって $\bar{a}=(1\ 2\ 3\ 4)$，$\bar{b}=(2\ 3\ 4)$，また $c=ab^{-1}=(1\ 4)(2\ 8)(3\ 5)(6\ 7)$ とすると，$\bar{c}=(1\ 4)$ である．したがって $\{\bar{x} \mid x \in G\}$ は $\{1,2,3,4\}$ 上対称群 S_4 である．

問 4.2　G を Ω 上 t 重可移とする．$\Omega-\{1\}$ の任意の $i_2, i_3, \cdots, i_t$ に対して，G に $x=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ 1 & i_2 & \cdots & i_t & \cdots \end{pmatrix}$ が存在し，$x \in G_1$ であるから，G_1 は $\Omega-\{1\}$ 上 $t-1$ 重可移である．

逆に任意の $i_1, i_2, \cdots, i_t$ に対して，$1^a=i_1$ である元 $a \in G$ が存在する．さらに $i_2^{a^{-1}}, \cdots, i_t^{a^{-1}} \subseteqq \Omega-\{1\}$ に対して，G_1 に $b=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ 1 & i_2^{a^{-1}} & \cdots & i_t^{a^{-1}} & \cdots \end{pmatrix}$ が存在する．したがって $ba=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ 1 & i_2^{a^{-1}} & \cdots & i_t^{a^{-1}} & \cdots \end{pmatrix}\begin{pmatrix} 1 & i_2^{a^{-1}} & \cdots & i_t^{a^{-1}} & \cdots \\ i_1 & i_2 & \cdots & i_t & \cdots \end{pmatrix}=\begin{pmatrix} 1 & 2 & \cdots & t & \cdots \\ i_1 & i_2 & \cdots & i_t & \cdots \end{pmatrix}$ となり，G は t 重可移である．

問 4.3　G が Ω 上 2 重可移とすると，$a=(1\ 2)\cdots$ なる元が存在する．このとき a の適当なべきは位数 2 の元となる．したがって a を位数 2 としてよい．$H=\langle a\rangle$ とおき，a が動かす文字 i をとる．$a \notin G_i$ だから，系4.8より　$G=G_i+G_i a G_i=G_i H G_i$

である．逆に $G=G_iHG_i$, $H=\langle a\rangle$ は位数2とすると，$G=G_i\cup G_iaG_i$ となり，系4.8 より Ω 上2重可移となる．

§ **5.** (41ページ) **問 5.1** 問1.4でみたように，$c=a^2=b^2=(1\ 3)(2\ 4)(5\ 7)\cdot(6\ 8)$ は，G のただ1つの位数2の元で，互換をもつ G の元は c のみである．$\langle c\rangle\lhd G$ で，注5.2より $\langle c\rangle$-軌道上可移であり，$(1,2)^c=(2,1)$ より G は Γ 上可移である．

問 5.2 定理5.8より，$\sum_{x\in G}\binom{\alpha_1(x)}{3}=\frac{m\cdot|G|}{3!}$. 固定点を3個もつ G の元は，単位元のみで，$|G|=2n$ より $\frac{n(n-1)(n-2)}{3!}=\frac{m\cdot 2n}{3!}$, $m=\frac{(n-1)(n-2)}{2}$ である．

問 5.3 $\sum_{x\in G}\binom{\alpha_1(x)}{3}=\frac{|G|}{3!}$, $\sum_{x\in G}\frac{\alpha_1(x)(\alpha_1(x)-1)(\alpha_1(x)-2)}{3!}=\frac{|G|}{3!}$, $\sum_{x\in G}(\alpha_1(x)^3-3\cdot\alpha_1(x)^2+2\cdot\alpha_1(x))=\sum_{x\in G}\alpha_1(x)^2-3\cdot 2\cdot|G|+2\cdot|G|=\sum_{x\in G}\alpha_1(x)^3-4|G|=|G|$, $\sum_{x\in G}|F(x)|^3=5\cdot|G|$.

問 5.4 $N=N_G(U)_{(F(H))}$ とおく．$N^{F(H)}\leqq N_G(H)^{F(H)}$. $^\forall x\in N_G(H)$ に対して $U^x\leqq H$. 仮定より $U^x=U^y$ なる $y\in H$ が存在する．$xy^{-1}\in N_G(U)\cap N_G(H)$. したがって $xy^{-1}\in N_G(U)_{(F(H))}=N$, $(xy^{-1})^{F(H)}=x^{F(H)}\cdot(y^{-1})^{F(H)}=x^{F(H)}$ より，$x^{F(H)}\in N^{F(H)}$, $N^{F(H)}=N_G(H)^{F(H)}$.

§ **6.** (49ページ) **問 6.1** $G=H+H(1\ 2)+H(1\ 3)+H(1\ 4)+H(1\,2\,4)+H(1\ 4\ 2)$, $G=K+K(1\ 2)+K(1\ 3)+K(1\ 4)+K(1\ 2\ 4)+K(1\,4\,2)$ である．$(1\ 2)(3\ 4)$ は G/H 上 $(H\ H(1\ 3))(H(1\ 2)\ H(1\ 2\ 4))$, G/K 上1である．$(1\ 2\ 3\ 4)$ は G/H 上 $(H(1\ 2)\ H(1\ 4\ 2)\ H(1\ 2\ 4)\ H(1\ 4))$, G/K 上 $(K\ K(1\ 3))\cdot(K(1\ 2)\ K(1\ 4\ 2))(K(1\ 4)\ K(1\ 2\ 4))$ である．

問 6.2 $H=\langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle$, $K=\langle(1\ 2),\ (3\ 4)\rangle$ は共に4元群である．S_4 の H による置換表現の核は H で，K による置換表現は忠実である．

問 6.3 G の H による置換表現の核を N とすると，G/N は n 次の可移置換群と同型である．

問 6.4 $|i^G|/|i^P|=(|G|/|G_i|)/(|P|/|P_i|)=(|G|/|P|)/(|G_i|/|P_i|)$. $|i^G|(|G_i|/|P_i|)=|i^P|(|G|/|P|)$. したがって $p^m\,|\,|i^P|$. 特に $(|G_i|/|P_i|,p)=1$ のとき $|i^P|=p^m$ である．

§ **7.** (58ページ) **問 7.1** S_4, A_4 は系7.7より原始的である．これ以外の可移群は位数が4または8で，次数4の2-群であるから，系7.11より非原始的である．

問 7.2 G を $\Omega=\{1,2,\cdots,5\}$ 上の原始置換群とする．系7.6より Ω 上の可移群は

原始的である．Gは位数5の元をもつから，$a=(1\ 2\ 3\ 4\ 5)\in G$ としてよい．Gにおける 5-シロー部分群の個数 $=1+5k=|G:N_G(\langle a\rangle)|$ より1または6個である．6個とすると $A_5>\langle a\rangle$ で，6個の 5-シロー部分群が生成する群は A_5 の正規部分群になり，A_5 は単純群であるから，$G=S_5$ または A_5 である．

Gの 5-シロー部分群は $\langle a\rangle$ のみとする．$G\geqq\langle a\rangle$ である．系 7.18 より $C_G(\langle a\rangle)=\langle a\rangle$．$G/\langle a\rangle\leqq \mathrm{Aut}\ (\langle a\rangle)$ で $\mathrm{Aut}\ (\langle a\rangle)$ の元は $a\mapsto a^i$ $(i=1,2,3,4)$ により決まるから，$|\mathrm{Aut}\ (\langle a\rangle)|=4$ である．$x\in G-\langle a\rangle$ に対して，$a^x=a^r$, $r=2,3$ または4で，$|\mathrm{Aut}\ (\langle a\rangle)|=4$ より，xの位数は2または4である．$|\Omega|=5$ より $F(x)\ni 1$ としてよい．

$a^x=a^2$ とすると，$x=\begin{pmatrix}1&2&3&4&5\\1&3&5&2&4\end{pmatrix}=(2\ 3\ 5\ 4)$，$a^x=a^3$ とすると，$x=\begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}=(2\ 4\ 5\ 3)$，$a^x=a^4$ とすると，$x=\begin{pmatrix}1&2&3&4&5\\1&5&4&3&2\end{pmatrix}=(2\ 5)(3\ 4)$ である．よって $G=\langle(1\ 2\ 3\ 4\ 5)\rangle$，$\langle(1\ 2\ 3\ 4\ 5),\ (2\ 3\ 5\ 4)\rangle$，$\langle(1\ 2\ 3\ 4\ 5),(2\ 5)(3\ 4)\rangle$ またはGと共役な群である．

問 7.3　(1)　$1^x=1^{x'}=i$ とし，任意の $j^x\in\Delta_s(1)^x$ をとる．$xx'^{-1}\in G_1$, $j^{xx'^{-1}}\in\Delta_s(1)$より　$j^x\in\Delta_s(1)^{x'}$, $\Delta_s(1)^x\subseteqq\Delta_s(1)^{x'}$である．同様にして $\Delta_s(1)^x=\Delta_s(1)^{x'}$である．$i\in\Delta_s(1)$, $1^{a_i}=i$ とする．$i^{a_iG_i}=i^{a_ia_i^{-1}G_1a_i}=i^{G_1a_i}=\Delta_s(1)^{a_i}=\Delta_s(i)$である．

(2)　(i)　Gを非原始的とし，Δを1を含む自明でないGの非原始ブロックとする．定理7.4よりΔは $G_{(\Delta)}$-軌道で，$G_1\lneqq G_{(\Delta)}$ より $\Delta\supseteqq\Delta_s(1)$ である G_1-軌道 $\Delta_s(1)$が存在する．いま $\Delta\cap\Delta_s(i)\neq\phi$ とする．$1^x=i, x\in G$ をとる．$\Delta_s(i)=\Delta_s(1)^x\subseteqq\Delta^x$ したがって　$\phi\neq\Delta\cap\Delta_s(i)\subseteqq\Delta\cap\Delta^x$　となり $\Delta=\Delta^x\supseteqq\Delta_s(i)$ である．いま $j\in\Omega-\Delta$ をとり $j\in\Delta_s(i)$ をとる．上より $\Delta\cap\Delta_s(i)=\phi$ となり，1とiはΔ_sで結ばれない．

(ii)　Δ_sにより結ばれない2点が存在するとする．Gは可移だから，1とiがΔ_sで結ばれないとしてよい．1とΔ_sで結ばれているΩの点の集合をΓとし，$\Delta=\bigcup_{j\in\Gamma}\Delta_s(j)$とおく．このとき $\Delta\cap\Delta_s(i)=\phi$ より $\Delta\subsetneqq\Omega$ である．また $|\Delta|=1$ とすると，$|\Delta_s(1)|=1$ となり，定理 7.12 より $G_1=1$ となり仮定に反する．したがって $|\Delta|\gneqq 1$ である．

いま $\Delta\cap\Delta^x\neq\phi$ とする．$\Delta_s(j)\subseteqq\Delta$, $\Delta_s(j)^x\cap\Delta\neq\phi$ が存在する．任意の $\Delta_s(j')\subseteqq\Delta^x$ をとる．1と j^x および j^x と j' は Δ_s で結ばれ，$\Delta_s(j')\subseteqq\Delta, \Delta=\Delta^x$ となり，ΔはGの自明でない非原始ブロックである．

§8. (67 ページ)　**問 8.1**　$G_{1234}\neq 1$ であれば，Gは3-巡回置換 (5 6 7) または互換，たとえば (5 6) をもち，系8.3より $G=S_7$ またはA_7である．$G_{1234}=1$

とする．G_{123} は $\{4,5,6,7\}$ 上可移で，$G_{1234}=1$ よりGは (2, 2) 型の元たとえば $a=(4\ 5)(6\ 7)$ をもつ．Gは4重可移だから，任意の異なる $i,j,k,l\in\Omega$ に対して，$x=\begin{pmatrix}4 & 5 & 6 & 7 & \cdots\\ i & j & k & l & \cdots\end{pmatrix}$ がGに存在し，$a^x=(i\ j)(k\ l)\in G$ である．したがって補題 3.10 より $G\geqq A_7$ で $G_{1234}=1$ に反する．

問 8.2　Gは4重可移だから，$N_G(P)^{F(P)}$ は4重可移である．問8.1より $N_G(P)^{F(P)}=S_7$ またはA_7である．いま $N_G(P)^{F(P)}=S_7, F(P)=\{1,2,\cdots,7\}$ とする．$a\in N_G(P)$, $a=(1)(2)(3)(4)(5)(6\ 7)\cdots$ なる元が存在して，$\langle a, P\rangle\leqq G_{1234}$, $|\langle a, P\rangle|=2\cdot|P|\cdot k$ となり，Pが G_{1234} の 2-シロー部分群であることに反する．したがって $N_G(P)^{F(P)}=A_7$ である．

問 8.3　$F(P)=\{1,2,\cdots,7\}$ とし，いま P が $a=(1)(2)\cdots(7)(8\ 9\ 10\ 11)\cdots$ (巡回表示) なる元をもつとする．$P-\{1\}$ の元は $\Omega-F(P)$ 上に固定点をもたないから，$a^2\neq 1$ より a は互換をもたないし，$F(a^4)\supsetneqq\{1, 2, \cdots, 11\}$ より $a^4=1$ となり a は $\Omega-F(P)$ 上 4-巡回置換のみの積である．$a\in N_G(G_{8\,9\,10\,11})$ より，補題 8.10 を用いて ($H=\langle a\rangle$, $N=G_{8\,9\,10\,11}\lhd\langle a, G_{8\,9\,10\,11}\rangle$ とする) $a\in N_G(Q)$ なる $G_{8\,9\,10\,11}$ の 2-シロー部分群Qが存在する．PとQ は G-共役だから，$|F(Q)|=7$ で問 8.2 より $N_G(Q)^{F(Q)}=A_7$ である．したがって $a^{F(Q)}=(8\ 9\ 10\ 11)(i\ j)(k)$ となり矛盾，すなわち $P-\{1\}$ の元はすべて位数が2で，Pは基本可換群である．

問 8.4　a' をPの中心の位数2の元とする．Pは Ω上可移であるから，$F(a')=F(P)$ である．Gは4重可移であるから，a' と共役な元 $a=(1\ 2)\cdots$ (巡回表示) が存在する．

任意の $i_1, i_2\ (\neq)\in F(a)$ に対して，P' を $G_{12i_1i_2}$ の 2-シロー部分群とする．Gは4重可移だから，G_{1234} と $G_{12i_1i_2}$ は共役で，したがって P' はPと共役で $P'\trianglelefteq G_{12i_1i_2}$ である．これより P' は $G_{12i_1i_2}$ のただ1つの 2-シロー部分群となり $a\in N_G(P')$ で，問8.2より $N_G(P')^{F(P')}=A_7$ である．これより $a^{F(P')}=(1\ 2)(i_1)(i_2)\cdot(i_3)(k\ l)$ となり，この方法により，$F(a)$ の任意の2点 i_1, i_2 に対して a の互換 $(k\ l)$ ($\neq(1\ 2)$) が一意的に決まる．

この $F(a)$ の2点 i_1, i_2 から互換 $(k\ l)$ ($\neq(1\ 2)$) への写像をφとする．$\varphi(j_1, j_2)=\varphi(i_1, i_2)=(k\ l)$ とする．$P'\leqq G_{12j_1j_2}\cap G_{12kl}$ より j_1, $j_2\in\{i_1, i_2, i_3\}$ である．逆に $\varphi^{-1}((k\ l))$ は，同様にして $\{\{i_1, i_2\}, \{i_1, i_3\}, \{i_2, i_3\}\}$ となる．したがってaの (1 2) 以外の互換の数は，$|F(a)|=7$ より，$\frac{1}{3}\binom{7}{2}=7$ となり，$n=2+7+2\times 7=23$ である．

§9.（76 ページ） **問 9.1** $GF(q^n)$ の加法群 $GF(q^n)^+$ は，$GF(q)$ 上の n 次元ベクトル空間である．いまその基 $\{v_1, v_2, \cdots, v_n\}$ をとる．乗法群 $GF(q^n)^\#$ は，位数 q^n-1 の巡回群 $\langle\rho\rangle$ である．いま写像 $\bar{\rho}:GF(q^n)^+\to GF(q^n)^+, v\mapsto \rho v$ をとると $\bar{\rho}$ は $GF(q^n)^+$ の線形写像で，$\{\rho v_1, \rho v_2, \cdots, \rho v_n\}$ は $GF(q)$ 上1次独立より，$GF(q^n)$ の基であるから，$\bar{\rho}\in GL(n,q)$ である．また $v^{\bar{\rho}^k}=v$ であれば，$\rho^k v=v$，$\rho^k=1$ となり $|\langle\bar{\rho}\rangle|=q^n-1$ である．またこれより $\langle\bar{\rho}\rangle_{v_1}=1$ で $|v_1^{\langle\bar{\rho}\rangle}|=|\langle\bar{\rho}\rangle|=q^n-1$ となり，$\langle\bar{\rho}\rangle$ は $GF(q^n)-\{0\}$ 上可移，したがって $\langle\bar{\rho}\rangle$ は $V(n,q)-\{0\}$ 上可移である．

問 9.2 W_1，W_2 を任意の m 次元部分ベクトル空間とし，その基をそれぞれ $\{u_1, \cdots, u_m\}$, $\{v_1, \cdots, v_m\}$ とする．V の基 $\{u_1, \cdots, u_m, \cdots, u_n\}$, $\{v_1, \cdots, v_m, \cdots, v_n\}$ をとり，$\sigma\in GL(V), u_i^\sigma=v_i$ $(i=1,2,\cdots,n)$ をとる．このとき $u_i^\tau=v_i$ $(i=1,2,\cdots,n-1)$, $u_n^\tau=(\det\sigma)^{-1}u_n$ をとると，$W_1^\tau=W_2$ で $\det\tau=(\det\sigma)(\det\sigma)^{-1}=1$ となり，$\tau\in SL(V)$ である．

問 9.3 （1） $V(n,q)$ および $GF(q)$ を加法群とみなすとき，f は V から $GF(q)$ への準同型写像である．したがって $V/\ker f\cong GF(q)$ である．$\ker f$ は $GF(q)$ 上のベクトル空間であり，$\dim GF(q)=1$ であるから，$\dim\ker f=n-1$ である．逆に超平面 U の基を $\{u_1, \cdots, u_{n-1}\}$ とし，これを含む V の基 $\{u_1, \cdots, u_{n-1}, u_n\}$ をとる．線形写像 $f: V\to GF(q)$, $u_i^f=0$ $(i=1,\cdots,n-1)$, $u_n^f=1$ は $\ker f=U$ である線形関数である．

（2） $V=U+\langle u'\rangle$, $u'^f=\lambda\ (\neq 0)\in GF(q)$ である．いま $u=\lambda^{-1}u'$ とおくと，$V=U+\langle u\rangle$, $u^f=1$ である．$v_0=u-u^\tau$ とおくと，$v_0\in U$ で，任意の $v=v'+\mu u\in V(v'\in U,\ \mu\in GF(q))$ に対して，$v^f=v'^f+(\mu u)^f=\mu$ で，$v^\tau=v'^\tau+(\mu u)^\tau=v'^\tau+\mu(u^\tau)=v'+\mu(u-v_0)=v'+\mu u-\mu v_0=v-v^f v_0$ である．

（3） $\ker f=U$ は V の超平面で，$V=U+\langle u\rangle$ である．$v^\tau=v-v^f v_0$ より，τ は V の線形写像で，$v^\tau-v=-v^f v_0\in U$，また $v\in U$ に対して $v^\tau=v$ である．さらに $u^\tau=u-u^f v_0\notin U$ より τ は正則であるから，τ は V の移換である．

（4） V の基を $\{v_1, \cdots, v_n\}$ とし，このうちの v_j を除く $n-1$ 個の基で生成される超平面を U_j とする．定理 9.2 の $a_{ij}(\alpha)$ をとると，任意の $v=\sum_{i=1}^{n}\lambda_i v_i\in V$ に対して，$v^{a_{ij}(\alpha)}=v+\alpha\lambda_i v_j$ で，$a_{ij}(\alpha)$ は U_j に関する移換である．逆に，移換は明らかに $SL(V)$ の元であるから，定理 9.2 より移換は $SL(V)$ を生成する．

§10.（89 ページ） **問 10.1** H は位数 $p^{r\cdot\frac{n(n-1)}{2}}$ の群で，位数より，$PSL(n,p^r)$, $PGL(n,p^r)$ の p-シロー部分群である．

問 10.2 同一直線上にある3点を $[v_1]$, $[v_2]$, $[\lambda_1 v_1 + \lambda_2 v_2]$ とし，$a \in GL(V)$ が $v_1{}^a = \mu_1 v_1$, $v_2{}^a = \mu_2 v_2$, $(\lambda_1 v_1 + \lambda_2 v_2)^a = \mu_3(\lambda_1 v_1 + \lambda_2 v_2)$ とする．このとき $(\lambda_1 v_1 + \lambda_2 v_2)^a = \lambda_1 \mu_1 v_1 + \lambda_2 \mu_2 v_2$ より $\mu_1 = \mu_2 = \mu_3 = \mu$ となる．任意の $[\lambda_1' v_1 + \lambda_2' v_2]$ に対して $(\lambda_1' v_1 + \lambda_2' v_2)^a = \mu(\lambda_1' v_1 + \lambda_2' v_2)$ となり，$[\lambda_1' v_1 + \lambda_2' v_2]^{[a]} = [\lambda_1' v_1 + \lambda_2' v_2]$ である．

$[v_1]$, $[v_2]$ に対して，$v_1{}^{\sigma_\theta} = v_1$, $v_2{}^{\sigma_\theta} = v_2$ である $[\sigma_\theta] \in P\Gamma L(V)$ をとると，$(v_1 + v_2)^{\sigma_\theta} = v_1 + v_2$ である．このとき $\lambda^\theta \neq \lambda$ である λ をとると，$(v_1 + \lambda v_2)^{\sigma_\theta} = v_1 + \lambda^\theta v_2$, $[v_1 + \lambda v_2]^{[\sigma_\theta]} \neq [v_1 + \lambda v_2]$ である．

問 10.3 定理 10.6 より，$PGL(2, K)$ は $PG(1, K)$ 上3重可移で，問 10.2 より3点の安定化群は1である．

問 10.4 $(PSL(2, q), PG(1, q))$ を $(L_2(q), \Omega)$, $\Omega = \{\infty, 0, 1, \cdots, \omega^{q-2}\}$, $GF(q)^* = \langle \omega \rangle$ とみなす．このとき系 10.9 より $H = G_{\infty 0} = \langle \sigma \rangle$, $\sigma : \xi \mapsto \omega^2 \xi$, $|H| = q - 1/(2, q-1)$, $F(H) = \{\infty, 0\}$ である．$N_G(H)^{F(H)}$ は2重可移より，$N_G(H) = \langle \sigma, \tau \rangle$, $\tau : \xi \mapsto -\xi^{-1}$ で，$|N_G(H)| = 2 \cdot |H|$ となる．ここで $\tau^{-1}\sigma\tau : \xi \mapsto -\xi^{-1} \mapsto -\omega^2 \xi \mapsto \omega^{-2}\xi$ より $\sigma^\tau = \sigma^{-1}$ となり，$N_G(H)$ は2面体群である．

§ **11.** (95 ページ) **問 11.1** ベクトル0の安定化群は $GL(n, q)$ だから $A(n, q)$ は V 上2重可移である．T についてはみやすい．

問 11.2 P は位数 p の可移群で，$N_G(P)$ の正則正規部分群である．$x \in N_G(P) - P$ で $|F(x)| \geqq 2$ とすると，$a(\neq 1) \in P$ で $C_G(a) \ni x$ なる a が存在する．このとき $\langle a \rangle = P$ より $x \in C_G(P)$ となり，系 11.8 より矛盾，したがって $|F(x)| = 0$ または1である．$|F(x)| = 0$ とすると x は異なる長さの巡回成分をもち，$x^r \neq 1$ で $|F(x^r)| \geqq 2$ となり矛盾，$|F(x)| = 1$ である．

問 11.3 $\bar{G}$ の部分群 $\{\varphi(1, b) \mid b \in G\}$ は G 上の置換群として，G^* に同値でしたがって $\bar{G}$ は G 上可移である．

（1）$\varphi(a, b) \cdot \varphi(c, d) = \begin{pmatrix} a_i \\ a^{-1}a_i b \end{pmatrix} \begin{pmatrix} a_i \\ c^{-1}a_i d \end{pmatrix} = \begin{pmatrix} a_i \\ c^{-1}a^{-1}a_i bd \end{pmatrix} = \begin{pmatrix} a_i \\ (ac)^{-1}a_i bd \end{pmatrix} = \varphi(ac, bd)$ より，写像 $f : G \times G \to \bar{G}$, $(a, b) \mapsto \varphi(a, b)$ は準同型である．$(a, b) \in \ker f \Leftrightarrow \varphi(a, b) = 1 \Leftrightarrow$ 任意の $a_i \in G$ に対して $a_i = a^{-1}a_i b$ である．ここで $a_i = 1$ にとり $1 = a^{-1} \cdot 1 \cdot b$ したがって $a = b$, $a_i = a^{-1}a_i a$ となり $a \in Z(G)$ となる．これより $\ker f = \{(a, a) \mid a \in Z(G)\}$, $|\bar{G}| = |G|^2/|Z(G)|$ である．

（2）$\bar{G}$ における $1 \in G$ の安定化群 $\bar{G}_1 = \{\varphi(a, b) \mid 1 = a^{-1}b\} = \{\varphi(a, a) \mid a \in G\}$ である．$a_i, a_j \in G$ に対して，a_i と a_j が共役である，すなわち $x^{-1}a_i x = a_j$ である

$\Leftrightarrow a_i^{\varphi(x,x)}=a_j$ より $\bar{G}$ の階数は $\bar{G}$ の共役類の数に等しい.

§ **12.**（100ページ） **問 12.1** MをGの極大部分群とし，GのG/M上の置換表現φを考える. G/M の1点Mの G^φ における安定化群は M^φ で，M^φ は G^φ の極大部分群であるから，G^φ は原始的な可解群である．定理 12.4(2) より G^φ の極小正規部分群は，正則な基本可換群で，位数を p^r（pは素数）とすると，$|G/M|=p^r$ である.

問 12.2 任意の $i,j(\neq)\in\Omega$ に対して，$|G_i|=n-1$, $G_i\cap G_j=1$ より，$|\bigcup_{i=1}^{n}G_i|=\sum_{i=1}^{n}|G_i-\{1\}|+1=n(n-2)+1$, $|N-\{1\}|=|G|-|\bigcup_{i=1}^{n}G_i|=n(n-1)-(n(n-2)+1)=n-1$ である. $a(\neq 1)\in N$ をとり，$1^a=i$ とする. G_1 は位数より $\Omega-\{1\}$ 上正則で，任意の $j\in\Omega-\{1,i\}$ に対して，$i^x=j$, $x\in G_1$ が存在する．このとき $1^{a^x}=j$ で $F(a^x)=\phi$ より $a^x\in N$ である. $G=G_1+G_1x_2+\cdots+G_1x_n$, $1^{x_i}=i$ とすると，Nの元は $G_1, G_1x_2,\cdots,G_1x_n$ にちょうど1つずつ含まれる.

任意の $a,b\in N$ に対して，$F(ab)\ni i$ とする. $i^x=1$ なる $x\in G$ が存在する. $a^x,b^x\in N$, $F(a^xb^x)\ni i^x=1$, $a^xb^x\in G_1$, $a^x\in G_1(b^x)^{-1}$ となり上より，$a^x=(b^x)^{-1}=(b^{-1})^x$, $a=b^{-1}$, $ab=1$, したがって $ab\in N$ となりNはGの部分群となる．これよりNは正規部分群になり，定理 12.4，定理 12.5 (1) よりNは基本可換群である.

問 12.3 N をGの非原始正規部分群とする. N が正則であれば，定理 12.5 (1) よりNは基本可換群でnは素数べきである．正則でないとNは$\frac{3}{2}$重可移で，定理 11.14 より Frobenius 群である．このとき Frobenius 核はGの正則正規部分群で，nは素数べきである.

問 12.4 Gを $\Omega=\{1,2,\cdots,6\}$ 上の原始置換群とする. $|F(G_1)|\geqq 2$ ならば，定理 7.12 よりGは正則で，位数6より $G_1=1$ はGの極大部分群でないから，Gは非原始的である．したがって $|F(G_1)|=1, G_1\neq 1$ である.

G_1 が $\{2,3,\cdots,6\}$ 上可移でないと，2つの軌道 $\{2,3\}$ と $\{4,5,6\}$ をもつとしてよい. $a=(4\ 5\ 6)\in G_1$ で $\langle a\rangle$ は G_1 の3-シロー部分群である．系 5.6 より $N_G(\langle a\rangle)$ は $F(a)=\{1,2,3\}$ 上可移で，$b=(1\ 2\ 3)\cdots\in N_G(\langle a\rangle)$ である．このとき $\{1,2,3\}$, $\{4,5,6\}$ は $\langle G_1,b\rangle$-軌道で，したがって $G_1\subsetneqq\langle G_1, b\rangle\subsetneqq G$ となり，系 7.5 に反する.

以上よりGはΩ上2重可移で，問 12.2 より $|G|\geqq 6\cdot 5$である．対称群 S_5は 5-群を6個もつから，G_1 は5-群を6個または1個もつ. 6個もつとGは可移だから，対称群 S_6 の5-群をすべて含み，これら5-群すべてより生成された群は交代群 A_6 の正規部分群となり，$G=S_6$ または A_6 で，原始的である.

G_1 が5-群Nをただ1つ含むと，$G_1\triangleright N$ で，$|\mathrm{Aut}\ N|=4$ より，$|G_1|=5\cdot 2$ また

は$|G_1| = 5 \cdot 4$ である．いま $N = \langle a \rangle, a = (2\ 3\ 4\ 5\ 6)$ とすると，$b = (3\ 4\ 6\ 5)$ または $b^2 = (3\ 6)(4\ 5) \in G_1$ である．G は2重可移だから b^2 と共役な $c = (1\ 2) \cdots \in G$ で，$c \in N_G(G_{1\,2})$ となる．$G_1 \triangleright \langle(2\ 3\ 4\ 5\ 6)\rangle$ より，$G_{1\,2}$ の位数2の元は b^2 のみで，b^2 と c は可換になり，$c = (1\ 2)(3\ 6)(4)(5)$ としてよい．このとき

$$G = \langle(1\ 2)(3\ 6)(4)(5),\ (1)(2\ 3\ 4\ 5\ 6),\ (1)(2)(3\ 4\ 6\ 5)\rangle$$

または

$$G = \langle(1\ 2)(3\ 6)(4)(5),\ (1)(2\ 3\ 4\ 5\ 6),\ (1)(2)(3\ 6)(4\ 5)\rangle$$

となるが，これは $PG(1,5)$ 上の $PGL(2,5)$，$PSL(2,5)$ である．

あ と が き

群論の知識なしには置換群の研究はできない．特に最近の有限群論の発展はめざましいものがある．しかしそれらの結果が，整理されて読み易い状態になるまでにはまだ多くの年月を要するものと思うし，そのときには置換群のとり扱いも変ってくるであろう．

第1章は本書に必要とする群論等の最小限の性質をあげたにすぎず，ぜひ下記の著書を読まれることをお勧めする．

［1］ 浅野啓三，永尾汎：群論（岩波書店，1965）

［2］ 鈴木通夫：群論上，下（岩波書店，1977，1978）

第2章は置換群特有の性質のうち最も基礎的なものをあげたが，その際下記の文献を参考にした．

［3］ 永尾汎：群とデザイン（岩波書店，1974）

［4］ 都筑俊郎：有限群と有限幾何（岩波書店，1976）

［5］ W. Burnside: Theory of groups of finite order (2nd ed.) (Cambridge, 1911)

［6］ B. Huppert: Endliche Gruppen I (Springer, 1967)

［7］ D. Passman: Permutation groups (Benjamin, 1968)

［8］ H. Wielandt: Finite permutation groups (Academic Press, 1964)

これらの著書もあわせて読まれるならば，置換群と関係のある広い知識が得られるであろう．

有限単純群の分類の完成にともない，2重可移群の分類問題も終る．特に4重可移群については，対称群，交代群および Mathieu 群のみであろう．第3章では Mathieu 群についていくつかの性質を述べたが，そのなかで Witt システムの一意性については

［9］ H. Lüneburg: Transitive Erweiterungen endlicher Permutationsgruppen (Springer, 1969)

によるものである．なおいくつかの2重可移群について書きたいと思ったが，そのためには本書の程度を越えた記述を必要とするので取り上げ得なかった．雑誌「科学」（岩波書店，1974年9月号）の“有限群論の現状”のなかに現在知られている（おそらくこれらのみであろう）正則正規部分群をもたない2重可移群の表がのせられているのでこれを引用させてもらう．

Gをn次の2重可移群とすると

（1） $G=S_n$，n次 （2） $G=A_n$，n次 （3） $PSL(n,q)\leqq G\leqq P\Gamma L(n,q)$, $n=(q^n-1)/(q-1)$ （4） $PSU(3,q^2)\leqq G\leqq P\Gamma L(3,q^2)$, $n=q^3+1$ （5） $S_z(q)\leqq G\leqq \mathrm{Aut}\, S_z(q)$，$n=q^2+1$ （6） $S_p(2m,2)$, $n=2^{m-1}(2^m\pm 1)$ （7） $G=R(q)$，$n=q^3+1$ （8） $G=PSL(2,11)$, $n=11$ （9） $G=A_7$，$n=15$ （10） $G=M_{11}$，$n=11$ （12） $G=M_{11}$，$n=12$ （13） $G=M_{12}$，$n=12$ （14） $G=M_{22}$，$n=22$ （15） $G=\bar{M}_{22}$，$n=22$ （16） $G=M_{23}$，$n=23$ （17） $G=M_{24}$，$n=24$ （18） $G=H_tS$，$n=176$ （19） Co_2，$n=276$.

これら2重可移群について，整理された分類がいつかはなされるものと期待している．

索　　引

セ

ソ

タ

チ

テ

ト

ナ

ニ

ハ

ヒ

フ

ヘ

ホ

マ

ミ

ム　モ

ユ

ヨ

リ　ル　レ

著者略歴

1929年（昭和４年）岡山県出身．昭和25年第六高等学校理科卒業，昭和28年大阪大学理学部数学科卒業．山口大学文理学部助教授を経て現在大阪教育大学教授．理学博士．

基礎数学選書 26　**有限置換群**　定価 2300 円

昭和 56 年 9 月 25 日　第 1 版印刷
昭和 56 年 9 月 30 日　第 1 版発行

著作者の了解により検印を省略いたします

著作者　大（おお）山（やま）　豪（つよし）
発行者　吉野達治
発行所　東京都千代田区四番町 8 番地
電話　東京　262—9166～9
株式会社　裳華房
印刷所　政弘印刷株式会社
製本所　株式会社　高陽堂

社団法人
自然科学書協会会員

本書の内容の一部あるいは全部を無断で複写複製（コピー）することは，法律で認められた場合を除き，著作者および出版社の権利の侵害となりますので，その場合は予め小社あて許諾を求めて下さい

ISBN4-7853-1128-2

Printed in Japan

■ 大学演習新書 ■

微分積分学　三村征雄編　定価 2,300 円

代数学と幾何学　三村征雄編　定価 2,200 円

微分方程式　矢野健太郎著　定価 2,200 円

解析学概論　矢野・石原共著　定価 2,400 円

ベクトル解析　矢野・石原共著　定価 2,500 円

函数論　辻・小松編　定価 2,400 円

応用数学 I　吉田・加藤共著　定価 2,600 円

数理統計　河田・丸山・鍋谷共著　定価 2,700 円

■ 数学選書 ■

1 線型代数学　佐武一郎著　定価 2,000 円

2 ベクトル解析　岩堀長慶著　定価 2,700 円

3 解析函数　田村二郎著　定価 1,800 円

4 ルベーグ積分入門　伊藤清三著　定価 2,600 円

5 多様体入門　松島与三著　定価 2,700 円

6 可換体論　永田雅宜著　定価 2,600 円

■ 基礎数学選書 ■

矢野 健太郎・国沢 清典・茂木 勇
石原 繁・岩堀 長慶 編集

1 積分　石原 繁著　定価 1,600 円

2 平面解析幾何学　矢野健太郎著　定価 1,700 円

3 微分　茂木 勇著　定価 2,000 円

4 立体解析幾何学　矢野健太郎著　定価 1,700 円

5 群と位相　横田一郎著　定価 2,500 円

6 線形空間　柴岡泰光著　定価 1,400 円

7 初等幾何学　清宮俊雄著　定価 1,700 円

8 待ち行列　鈴木武次著　定価 1,700 円

9 ベクトル解析　武藤義夫著　定価 2,200 円

10 群と表現　横田一郎著　定価 2,500 円

11 座標　栗田 稔著　定価 1,600 円

12 線形代数の基礎（上,下）　野水著・矢野訳　(上)2,100円・(下)2,300円

13 代数的整数論入門（上,下）　藤崎源二郎著　(上)1,800円・(下)1,700円

14 計量微分幾何学　松本 誠著　定価 1,800 円

15 現代数学と数学教育　森 毅著　定価 2,100 円

16 確率論入門　志村利雄著　定価 2,200 円

17 曲線と曲面の微分幾何　小林昭七著　定価 1,700 円

18 数字と数学記号の歴史　大矢・片野共著　定価 1,800 円

19 常微分方程式　鈴木七緒著　定価 2,200 円

20 いろいろな曲線と曲面　佐藤伊助著　定価 2,300 円

21 行列特論　草場公邦著　定価 2,400 円

22 複素数と関数　安岡善則著　定価 2,000 円

23 テンソル解析　田代嘉宏著　定価 2,500 円

24 線形代数と量子力学　竹内外史著　定価 1,900 円

25 現代微分幾何入門　野水克己著　定価 2,300 円

26 有限置換群　大山 豪著　定価 2,300 円